JOINT APPENDIX
VOLUME II

EXHIBIT 62

How does Tornado Cash work?

by Alex Wade & Michael Lewellen & Peter Van Valkenburgh
August 25, 2022

1. Introduction

In August 2022, the US Treasury's Office of Foreign Assets Control (OFAC) sanctioned Tornado Cash, adding 45 Ethereum addresses to the Specially Designated Nationals (SDN) List of sanctioned persons.

This document aims to help the reader understand what Tornado Cash is, how it works, and what, exactly, was sanctioned. But before we jump into Tornado Cash, let's review a few key concepts around Ethereum, smart contracts, and decentralization.

2. Background: What is Ethereum, who are its users, what is a smart contract?

Ethereum is a cooperatively-run, global, transparent database. Through mutual effort, participants from all over the world maintain Ethereum's public record of addresses, which reference both user accounts and smart contract applications. These records work together much like the user accounts and software of a modern desktop computer, except that Ethereum is:

- Cooperatively-run: Ethereum's fundamental operation comes from the collective effort of its participants

worldwide. No single party can make changes to how Ethereum works.

- Publicly-accessible: Anyone anywhere in the world can interact with Ethereum, its users, and its applications.
- Transparent: Anyone anywhere in the world can download and view all the information in Ethereum's database.

Anyone can be a user of Ethereum. Creating an account is simple, and does not require a phone number, email, or physical address. Instead, users install an application called a "wallet," which generates a unique identifier for that user called an "address" and a password-like number for authentication called a "private key." Much like a person with multiple email addresses, Ethereum's users can create and use as many addresses as they want. Unlike with email, however, Ethereum's users are not "customers" in the traditional sense. They are participants in a global computing system running on open-source software, which functions without third-party oversight. It is also important to note that Ethereum addresses controlled by the same user are not necessarily publicly linked to one another; they are simply unique identifiers that belong to the user who has the corresponding private key.

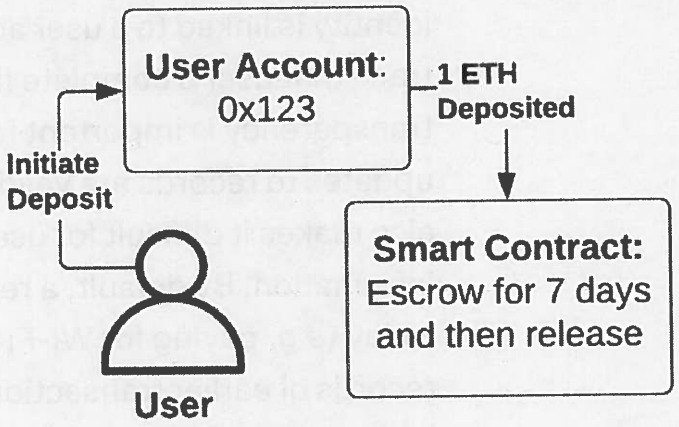
By sharing an address, users are able to receive tokens (*e.g.* crypto-assets like Ether) from anyone, anywhere in the world. Unlike a traditional payment service, sending and receiving tokens on Ethereum does not require an intermediary. Instead, the sender broadcasts their intent to transfer tokens, signs their message mathematically using the corresponding private key, and Ethereum's network collectively updates the global records of the sender and receiver addresses with the new balances. At no point in this process does a third party take custody of the tokens being transferred.

In addition to sending and receiving tokens, user accounts can interact with smart contracts, which are applications that extend the functionality of Ethereum. When developers program smart contracts, they decide what operations the smart contract will support and what rules those operations must follow. These rules and operations are written using code that is broadcast to Ethereum's network, just like the token transactions described above. Once a smart contract's code is added to Ethereum's records, it receives a unique address and can be interacted with by any user to automatically carry out the rules and operations it supports.

In essence, smart contracts are open-source applications that anyone can deploy to Ethereum. Just like the rest of Ethereum, smart contracts can be viewed and used by anyone, anywhere, and without relying on an intermediary.

Both people and smart contracts can have Ethereum addresses; the key difference is that when a person has an address they have the private key that controls any tokens sent to that address. That person will ultimately decide if and when any transactions are made with those tokens. When a smart contract has an address, the rules and operations written in the smart contract code control the tokens. They could be simple rules (*e.g.* automatically send the tokens back), or more complicated rules. There could be rules that include human operations and human decisions (*e.g.* send the tokens back if 3 out of 5 of these human-controlled addresses send a signed message saying they agree). The rules could also, however, be fully and permanently outside of any human being's control. In that case, so too are any tokens sent to that address until and unless the contract sends them back to some human according to the rules.

Ethereum Smart Contract Example: Timelocked Escrow



The User deposits 1 ETH token to be held in escrow for 7 days by the Smart Contract. After 7 days, the user can reclaim the tokens.

By default, smart contracts are immutable, which means they cannot be removed or updated by anyone once deployed. It is possible for the smart contract's developers to include (in the contract code) the ability to update functionality as a supported operation (*e.g.* this *human-controlled* address can rewrite the contract in the future). However, such an operation must be included in the smart contract's code prior to the smart contract's deployment (*i.e.* publication to the Ethereum network). Without the inclusion of updatability prior to deployment, a smart contract cannot be modified by anyone. It is also possible to revoke the ability to update functionality by transferring the permissions for this ability to a placeholder Ethereum address for which there is no corresponding private key. This placeholder is known as "the zero address." Once the ability to update a contract has been revoked, it cannot be reclaimed and the contract can no longer be changed.

Unlike traditional finance, Ethereum's records are completely transparent: anyone can download and view the balances and transaction history of its user accounts. Although user addresses are pseudonymous, if a real-world identity is linked to a user address, it becomes possible to trace that user's complete financial history. Ethereum's transparency is important for auditability (*e.g.* verifying that updates to records are valid). However, this transparency also makes it difficult for users to protect their personal information. By default, a record of a casual transaction today (*e.g.* paying for Wi-Fi at the airport) leads directly to records of earlier transactions, which may include any intimate, revealing, or sensitive transactions made by the same user long ago.

Among the many different applications smart contracts may support, they may also provide an avenue for users to regain the privacy they expect when interacting with financial systems. Central to that privacy is the use of smart contracts to break the public chain of records that would otherwise link your transaction today to every transaction you've ever made in the past. Enter Tornado Cash.

3. Tornado Cash: A smart contract application

Tornado Cash is an open source software project that provides privacy protection for Ethereum's users. Like many such projects, the name does not refer to a legal entity, but to several open source software libraries that have been developed over many years by a diverse group of contributors. These contributors have published and made Tornado Cash available for general use as a collection of smart contracts on the Ethereum blockchain.

As we will explain, some of these smart contracts have been sanctioned by OFAC. The core of Tornado Cash's privacy tools, however, make up a subset of the addresses sanctioned by OFAC: the Tornado Cash "pools." Each Tornado Cash pool is a smart contract deployed to Ethereum. Like other smart contracts, the pool contracts extend the functionality of Ethereum with specific operations that can be executed by any user of Ethereum according to the rules defined in the Tornado Cash contracts' code.

This section will describe how these pools work. In particular, it will describe the key innovation that enables these pools to function autonomously: an application of privacy-preserving mathematics known as "zero-knowledge cryptography."

Subsequent sections will describe the specific addresses sanctioned by OFAC, and what they do. An appendix at the end will list all of the sanctioned contracts and their salient features.

Tornado Cash Core Contracts: Pools

Tornado Cash pools are smart contracts that enable users to transact privately on Ethereum. When prompted by a user, pools will automatically carry out one of two supported operations: "deposit" or "withdraw." Together, these operations allow a user to deposit tokens from one address and later withdraw those same tokens to a different address. Crucially, even though these deposit and withdrawal events occur publicly on Ethereum's transparent ledger, any public link between the deposit and withdrawal addresses is severed. The user is able to withdraw and use their funds without fear of exposing their entire financial history to third parties.

In support of the deposit and withdrawal operations, these smart contracts encode strict rules that further define its functionality. These rules are automatically applied to the deposit and withdrawal operations to maintain a very important property shared by all Tornado Cash pools: **users can only withdraw the specific tokens they originally deposited.**

This property is enforced automatically for all the pool's operations, and ensures that Tornado Cash pools are entirely *non-custodial*. That is, a user who deposits and later withdraws tokens maintains total ownership and control over their tokens, even as they pass through the pool. At no point is the user required to relinquish control of their tokens to anyone.

A key principle of Tornado Cash pools is that a user's privacy is derived in large part from the simultaneous usage of the pool by many other users. If the pool had only a single user, it wouldn't matter that the link between the user's deposit and withdrawal addresses was severed: simple inference would make it obvious where the withdrawn tokens came from. Instead, pools are used by many users simultaneously. Think of it like a bank's safe deposit box room. Anyone can go and store valuables in a locked box in that room, and, assuming the locks are good, only the person with the key can ever get those valuables back. Security aside, however, this may or may not be privacy enhancing. If only one person is ever seen going into and out of the room, then we know any valuables in that room are theirs. If, on the other hand, many people frequently go into and out of the room, then we have no way of knowing who controls which valuables in which boxes. By guaranteeing the property that users can only withdraw tokens they originally deposited, many users can simultaneously use these pools with the assurance that no-one else will receive their tokens.

Traditionally, these assurances would be provided by a *custodial* service: a bank in the safe deposit box example, or a group of people running a "mixing service" in other common cryptocurrency arrangements. Mixing services like Blender.io directly accept tokens from their clients, aggregate and mix them, and then return the funds to their clients (often taking some fee in the process). During the intermediate aggregation and mixing stage, the funds in question are completely in the control of the operators of the mixing service and are commingled. At the final stage of the mixing process, a user would receive funds sourced directly from the myriad other users that also used the service.

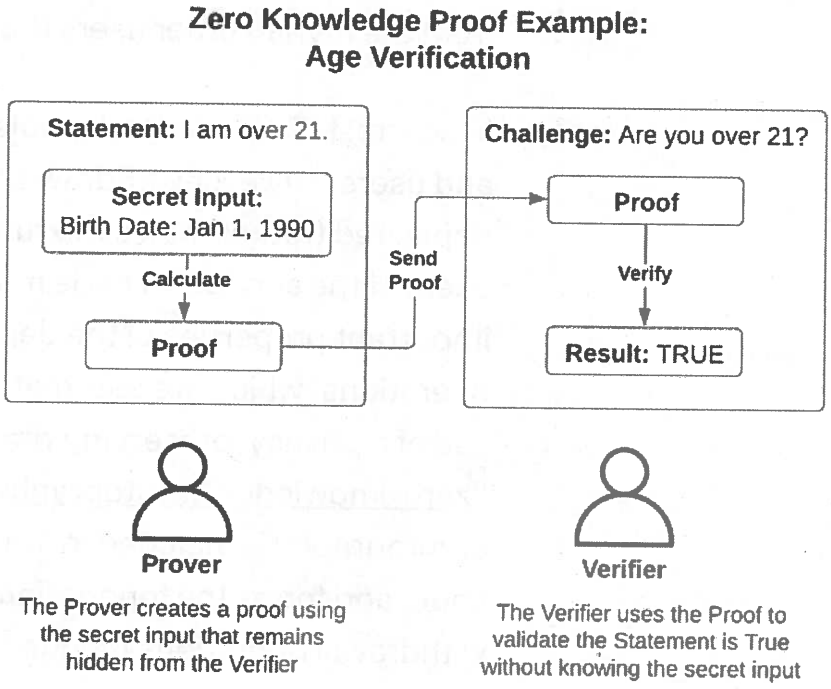
In contrast, Tornado Cash pools have no custodial operator, and users only ever withdraw the tokens they originally deposited (rather than a mixture of tokens from the other users of the service). This is made possible because of important properties of the deposit and withdrawal operations, which are automatically carried out through the use of a privacy-preserving branch of mathematics called "zero-knowledge cryptography." This zero-knowledge cryptography is included in Tornado Cash's smart contract code, and forms the foundation on which the deposit and withdrawal operations function.

Zero-Knowledge Proofs

To recall an earlier point, Ethereum is transparent: anyone can view the transaction history and balance of any user account. Likewise, anyone can view the interaction history, balance, and code of a smart contract application. If a user prompts a smart contract to perform an operation, this interaction becomes a fact that is forever recorded in Ethereum's public records and can be recalled and inspected by anyone. So how is it that a user can deposit into a Tornado Cash pool and later withdraw to a different

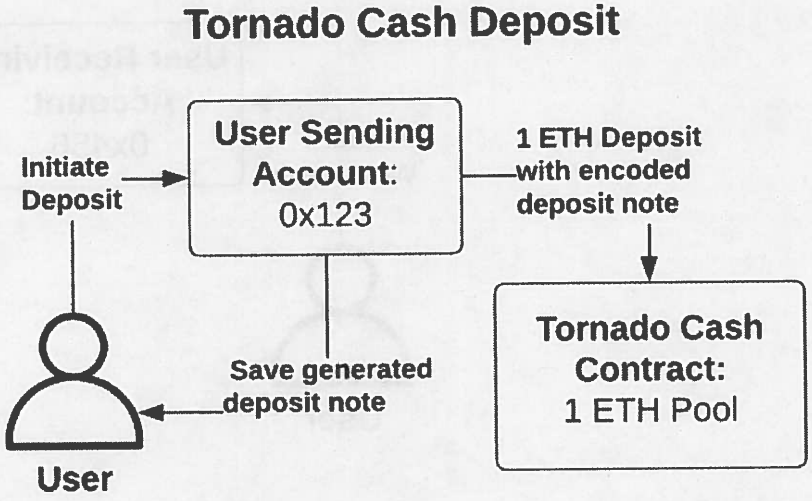
address without creating an obvious link to anyone observing Ethereum's public records?

The answer lies in *zero-knowledge proofs*. A zero-knowledge proof is a cryptographic method by which one party (the "prover") can prove to another party (the "verifier") that a given statement is true without the prover conveying any additional information apart from the fact that the statement is indeed true.



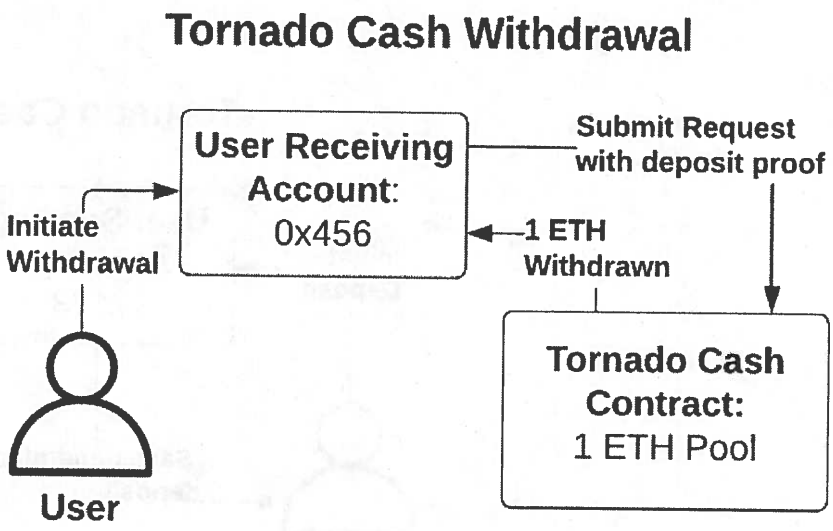
In the case of Tornado Cash, the "prover" is the user withdrawing tokens from the pool, while the "verifier" is one of the Tornado Cash pool contracts. When a user prompts the pool smart contract to withdraw their tokens, the user must supply the prompt with a zero-knowledge proof. The pool's code automatically checks the input proof, only processing a withdrawal if the proof is found to be valid. Exactly what statement is being proven by the user and how they create that proof is slightly more complicated, and requires a bit more detail on the deposit process.

Pool Deposit Process



When a user wants to deposit tokens, they first generate a "deposit note" (a long sequence of digits known only to the user). This is done privately on the user's own computer, and is never shared publicly. Next, the user prompts the Tornado Cash pool contract to process the deposit. Along with this prompt, the user supplies a hash (or encoded form) of their deposit note and the tokens for deposit. The pool smart contract automatically records the encoded note as a new entry in a public list of other users' encoded notes. At this point, the depositing user has completed the first part of the process, and retains the deposit note, which acts as a receipt to withdraw the tokens later.

Pool Withdrawal Process



When a user is ready to withdraw their tokens, they first split their deposit note in half. One side acts like a "secret," and the other acts like a "lock." After that, the user prompts the Tornado Cash smart contract to withdraw. Along with the prompt, the user supplies:

- A *hash* (or encoded form) of the "lock"
- A *zero-knowledge proof*, generated using the "secret" and the "lock"

The pool smart contract uses these inputs to automatically verify – that is, *prove* – the following:

1. That the zero-knowledge proof was generated using the "secret." It is the exact same "secret" that corresponds to one of the existing encoded notes in the pool's public list of encoded notes (*i.e.* proving that the tokens being withdrawn were previously deposited by someone).
2. That the same proof also corresponds to the encoded form of the "lock" supplied with the proof (*i.e.* proving that the person who is withdrawing them must be the same person who deposited them).

3. That the submitted "lock" has not been submitted previously (*i.e.* the deposit in question has not already been withdrawn).

Assuming the proof is verified, the pool smart contract automatically:

1. Sends the user their tokens.
2. Records the encoded "lock" in a public list of other users' encoded locks, ensuring the same tokens cannot be withdrawn again.

Crucially, the above operations are carried out while the following is never revealed: which specific encoded note the proof corresponds to (*i.e.* who, among all of Tornado Cash's depositors, is now withdrawing).

Can Tornado Cash be removed or updated? If so, by whom?

As stated previously, for most readers, *Tornado Cash* is synonymous with a core subset of the Tornado Cash smart contracts: the Tornado Cash pools. The vast majority of these contracts are immutable. That is, they have no ability to be updated or removed by anyone. A complete list of sanctioned, immutable Tornado Cash pools can be found in Appendix A.

Note that many of these pools had, at one point, an "operator" role. The operator role was originally held by 0xDD4c...3384, aka *Gitcoin Grants: Tornado.cash*, another sanctioned address. This role afforded its holder two permissions:

- updateVerifier: Used to update the "verifier" used by the smart contract. In essence, this permission could be used

to modify how the contract processed zero-knowledge proofs.

- changeOperator: Used to transfer the "operator" permission to another address, or revoke the "operator" permission entirely by transferring it to the zero address.

In May 2020, the updateVerifier permission was used in conjunction with the changeOperator permission as a final update to these Tornado Cash pools. This updated all pools' zero-knowledge proof processors to their final version, which incorporated the contributions of over 1,100 community participants. Additionally, this update revoked the "operator" permission by using changeOperator to transfer the permission to the zero address. In effect, the update performed in May 2020 cemented the community's preferences, and ensured no further changes could be made. Details on this process can be found here.

A handful of SDN-listed pools still have an "operator" permission. Of these, two belong to very old, now-unused versions of Tornado Cash. The remaining pools either have newer, immutable versions, or were used so little that they were likely overlooked during the May 2020 final update. Most of these remaining eight pools have never been used, and the ones that were used were only used once or twice within the past three years. A complete list of sanctioned, outdated Tornado Cash pools that retain the operator permission can be found in Appendix C.

Tornado Cash Auxiliary Contracts & Controls

Governance and TORN Token

The pool smart contracts represent the core of the Tornado Cash application, which remains immutable and uncontrolled by any party. However, OFAC's sanctions also

include auxiliary smart contracts that provide coordination mechanisms for the continued maintenance and use of Tornado Cash by its community. Several of these contracts are unused today, belonging to older versions of Tornado Cash. A complete list of OFAC-sanctioned smart contracts that relate to Tornado Cash's community maintenance can be found in Appendix B.

The SDN List includes two primary contracts still in use today:

- *Tornado Cash (Router)*: References a registry of up-to-date Tornado Cash pools, consistent with the current version of Tornado Cash. Users may *optionally* choose to interact with Tornado Cash pools via the Router contract, which ensures their deposit and withdrawal operations are processed using up-to-date code.

- *Tornado Cash (Relayer Registry)*: References a registry of operators providing relay-assisted withdrawal services to users of Tornado Cash. Users may *optionally* elect to process their withdrawals via a relayer, which may afford additional privacy.

Unlike the pool smart contracts, the Router and Relayer Registry support some updatable functionality. However, the permission to update these contracts is held not by a human, but by another smart contract. This smart contract, also known as *Tornado Cash: Governance*, defines the rules and operations that determine how the Router and Relayer Registry may be updated.

In short, *Tornado Cash: Governance* provides that updates to these smart contracts are processed at the behest of the community, which holds public votes to determine what updates should occur, and when. Any holder of TORN tokens may participate in these votes. TORN is an ERC20-

token built on Ethereum that is expressly used by the community to vote on governance proposals. Any user of Ethereum may purchase TORN tokens and participate in this process.

Note that while this process allows the wider Ethereum community to participate in the development and maintenance of Tornado Cash, *no part of this process allows for the update or removal of Tornado Cash pool smart contracts.* Additionally, participating in the *Tornado Cash: Governance* process is *entirely optional*: users can use Tornado Cash pools without any involvement, oversight, or interaction with the *Tornado Cash: Governance* process.

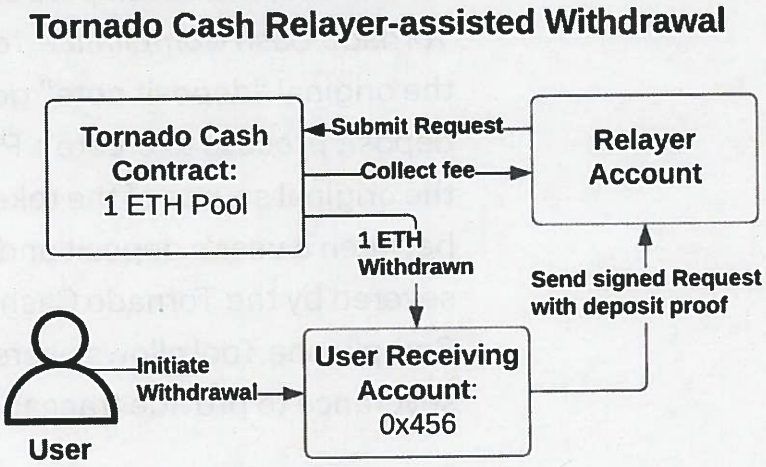
Although *Tornado Cash: Governance* and the TORN token contract are parts of the Tornado Cash software ecosystem, neither was added to OFAC's SDN List.

Relayers

As previously mentioned, "relayers" are independent operators that provide an *optional* service for Tornado Cash users.

By default, when users prompt the Tornado Cash pool contracts for withdrawal, the withdrawal account needs to already have Ether in order to pay the Ethereum network to process the smart contract's operations. However, sending Ether to the withdrawal account prior to withdrawal might create a link between the user's deposit and withdrawal accounts.

Relayers allow users to process withdrawals without needing to pre-fund their withdrawal accounts, which helps users maintain privacy when withdrawing.



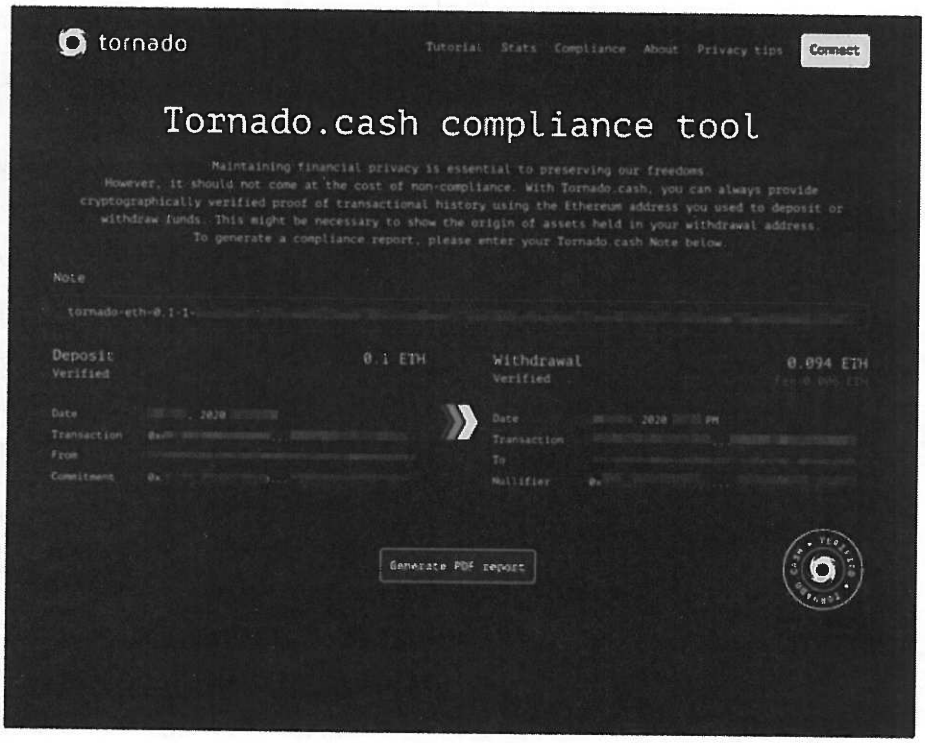
Users select a relayer from a public *Relayer Registry*, another sanctioned Tornado Cash smart contract. The user then uses their withdrawal account to sign a transaction authorizing the relayer-assisted withdrawal. The user sends this transaction to their selected relayer, who processes the withdrawal on their behalf, earning a fee in the process. Note that even though they process withdrawals on behalf of users, relayers never have custody over users' tokens; the smart contract ensures that withdrawn tokens are only ever sent to the user's withdrawal account.

OFAC has not specifically added any relayer addresses to the SDN List, but it has added the smart contract that contains a registry of relayers to the list.

Compliance Tool

Tornado Cash was built to enable Ethereum's users to reclaim their privacy. Rather than exposing their complete financial history, Tornado Cash gives users control over their personal information: both what is shared and with whom it is shared. However, maintaining privacy and preserving control over one's personal information does not need to come at the expense of non-compliance with legal obligations.

To this end, the developers of Tornado Cash created the *Tornado Cash Compliance Tool*. Users supply the tool with the original "deposit note" generated during the pool deposit process to create a PDF report that provides proof of the original source of the tokens. Although the public link between a user's deposit and withdrawal addresses was severed by the Tornado Cash pool contracts, the Compliance Tool allows users to selectively "undo" this severance to provide traceability to third parties.



The Compliance Tool is not a smart contract. However, just like the other software described in this article, the Compliance Tool is also not a service provided by Tornado Cash developers; it is an open-source tool that can be used by anyone.

Other Tornado Cash Smart Contracts and Addresses

Finally, two of the sanctioned addresses are donation addresses. These addresses were used in the past to raise

money in support of the development of the privacy software that powers Tornado Cash. While some person or entity does control tokens sent to these addresses, those tokens are not, to our knowledge, being mixed or re-routed for privacy purposes. They are merely a gift from the sender in support of software development efforts performed by the recipient. A complete list of donation addresses sanctioned by OFAC can be found in Appendix D.

In general, while a minority of the contracts listed by OFAC do retain elements of human control, none of them are critical to the basic operation of Tornado Cash's privacy tools, and none of them take control of user tokens. The core privacy tools – the pool contracts – are outside of any individual or group's control; they are simply widely distributed computer code that is executed by the Ethereum network according to strict and unalterable rules.

Summary

In summary:

- The Tornado Cash smart contracts allow users to deposit and later withdraw their tokens to another address.
- Even though anyone can observe users deposit or withdraw tokens, they are not able to determine which withdrawals correspond to which deposits.
- These operations are defined as smart contract code and are carried out automatically without any intermediary or third party.
- Users retain control of their funds the whole time, and are only able to withdraw the tokens they originally deposit.
- No one controls the operation of these Tornado Cash smart contracts and no one has the ability to change their

operation in the future.

- Some OFAC-identified addresses retain a level of human control. However, these addresses are not core to the operation of the privacy tools found at the immutable addresses and they can not exercise control over any user tokens.

Appendix: Categorization of sanctioned addresses

These appendices list all addresses sanctioned by OFAC. They have been categorized according to the function they provide in the context of the Tornado Cash application.

Included with each address listed is the following information:

- *Name:* A name by which the address can be referenced. Note that these names do not come from the Tornado Cash developers, they come from Etherscan: a third party service whose website can be used to display information on the current state of Ethereum. The names listed are intended to be a handy reference, and do not necessarily reflect the views of the community or the Tornado Cash developers.
- *Description:* A short description of what each address refers to.

A: List of immutable Tornado Cash pools

- 0x12D66f87A04A9E220743712cE6d9bB1B5616B8Fc
  - *Name:* Tornado.Cash: 0.1 ETH

- *Description:* A Tornado Cash pool that allows deposits and withdrawals in increments of 0.1 ETH.
- *Operator:* Revoked (operator set to zero address)

- 0x47CE0C6eD5B0Ce3d3A51fdb1C52DC66a7c3c2936
  - *Name:* Tornado.Cash: 1 ETH
  - *Description:* A Tornado Cash pool that allows deposits and withdrawals in increments of 1 ETH.
  - *Operator:* Revoked (operator set to zero address)
- 0x910Cbd523D972eb0a6f4cAe4618aD62622b39DbF
  - *Name:* Tornado.Cash: 10 ETH
  - *Description:* A Tornado Cash pool that allows deposits and withdrawals in increments of 10 ETH.
  - *Operator:* Revoked (operator set to zero address)
- 0xA160cdAB225685dA1d56aa342Ad8841c3b53f291
  - *Name:* Tornado.Cash: 100 ETH
  - *Description:* A Tornado Cash pool that allows deposits and withdrawals in increments of 100 ETH.
  - *Operator:* Revoked (operator set to zero address)
- 0xD4B88Df4D29F5CedD6857912842cff3b20C8Cfa3
  - *Name:* Tornado.Cash: 100 DAI
  - *Description:* A Tornado Cash pool that allows deposits and withdrawals in increments of 100 DAI.
  - *Operator:* Revoked (operator set to zero address)
- 0xFD8610d20aA15b7B2E3Be39B396a1bC3516c7144
  - *Name:* Tornado.Cash: 1000 DAI

- *Description:* A Tornado Cash pool that allows deposits and withdrawals in increments of 1000 DAI.
- *Operator:* Revoked (operator set to zero address)

- 0x07687e702b410Fa43f4cB4Af7FA097918ffD2730
  - *Name:* Tornado.Cash: 10000 DAI 2
  - *Description:* A Tornado Cash pool that allows deposits and withdrawals in increments of 10000 DAI.
  - *Operator:* None (functionality not included)
- 0x23773E65ed146A459791799d01336DB287f25334
  - *Name:* Tornado.Cash: 100000 DAI
  - *Description:* A Tornado Cash pool that allows deposits and withdrawals in increments of 100000 DAI.
  - *Operator:* None (functionality not included)
- 0x22aaA7720ddd5388A3c0A3333430953C68f1849b
  - *Name:* Tornado.Cash: 5000 cDAI
  - *Description:* A Tornado Cash pool that allows deposits and withdrawals in increments of 5000 cDAI.
  - *Operator:* Revoked (operator set to zero address)
- 0xBA214C1c1928a32Bffe790263E38B4Af9bFCD659
  - *Name:* Tornado.Cash: 50000 cDAI
  - *Description:* A Tornado Cash pool that allows deposits and withdrawals in increments of 50000 cDAI.
  - *Operator:* Revoked (operator set to zero address)
- 0x03893a7c7463AE47D46bc7f091665f1893656003
  - *Name:* Tornado.Cash: 50000 cDAI 2

- *Description:* A newer version of the 50000 cDAI Tornado Cash pool, which allows deposits and withdrawals in increments of 50000 cDAI.
- *Operator:* None (functionality not included)

- 0x2717c5e28cf931547B621a5dddb772Ab6A35B701
  - *Name:* Tornado.Cash: 500000 cDAI 2
  - *Description:* A Tornado Cash pool that allows deposits and withdrawals in increments of 500000 cDAI.
  - *Operator:* None (functionality not included)
- 0xD21be7248e0197Ee08E0c20D4a96DEBdaC3D20Af
  - *Name:* Tornado.Cash: 5000000 cDAI
  - *Description:* A Tornado Cash pool that allows deposits and withdrawals in increments of 5000000 cDAI.
  - *Operator:* None (functionality not included)
- 0x4736dCf1b7A3d580672CcE6E7c65cd5cc9cFBa9D
  - *Name:* Tornado.Cash: 100 USDC
  - *Description:* A Tornado Cash pool that allows deposits and withdrawals in increments of 100 USDC.
  - *Operator:* Revoked (operator set to zero address)
- 0xd96f2B1c14Db8458374d9Aca76E26c3D18364307
  - *Name:* Tornado.Cash: 1000 USDC
  - *Description:* A Tornado Cash pool that allows deposits and withdrawals in increments of 1000 USDC.
  - *Operator:* Revoked (operator set to zero address)
- 0x169AD27A470D064DEDE56a2D3ff727986b15D52B
  - *Name:* Tornado.Cash: 100 USDT

- *Description:* A Tornado Cash pool that allows deposits and withdrawals in increments of 100 USDT.
- *Operator:* Revoked (operator set to zero address)

- 0x0836222F2B2B24A3F36f98668Ed8F0B38D1a872f
  - *Name:* Tornado.Cash: 1000 USDT
  - *Description:* A Tornado Cash pool that allows deposits and withdrawals in increments of 1000 USDT.
  - *Operator:* Revoked (operator set to zero address)
- 0x178169B423a011fff22B9e3F3abeA13414dDD0F1
  - *Name:* Tornado.Cash: 0.1 WBTC
  - *Description:* A Tornado Cash pool that allows deposits and withdrawals in increments of 0.1 WBTC.
  - *Operator:* None (functionality not included)
- 0x610B717796ad172B316836AC95a2ffad065CeaB4
  - *Name:* Tornado.Cash: 1 WBTC
  - *Description:* A Tornado Cash pool that allows deposits and withdrawals in increments of 1 WBTC.
  - *Operator:* None (functionality not included)
- 0xbB93e510BbCD0B7beb5A853875f9eC60275CF498
  - *Name:* Tornado.Cash: 10 WBTC
  - *Description:* A Tornado Cash pool that allows deposits and withdrawals in increments of 10 WBTC.
  - *Operator:* None (functionality not included)

B: List of community-governed contracts

- 0xd90e2f925DA726b50C4Ed8D0Fb90Ad053324F31b
  - *Name:* Tornado.Cash: Router
  - *Description:* A contract that maintains a list of Tornado Cash pools, which can be used by users to route deposits and withdrawals to the correct Tornado Cash pool.
  - *Still in use*: Yes.
  - *Governance Controls:* No significant controls. The community may choose to withdraw any tokens sent to the Router, as the Router is not an intended recipient of tokens.
- 0x58E8dCC13BE9780fC42E8723D8EaD4CF46943dF2
  - *Name:* Tornado.Cash: Relayer Registry
  - *Description:* This contract allows anyone to register as a Tornado Cash relayer. Relayers provide an *optional* service for users to make gasless withdrawals.
  - *Still in use*: Yes.
  - *Governance Controls:* Updatable pending a community vote.
- 0x527653eA119F3E6a1F5BD18fbF4714081D7B31ce
  - *Name:* Tornado.Cash: Trees
  - *Description:* This contract holds a merkle tree (a kind of list) of all Tornado Cash deposit and withdrawal events.
  - *Still in use:* No, this is associated with an older version of Tornado Cash.
  - *Governance Controls:* Updatable pending a community vote.
- 0xCa0840578f57fE71599D29375e16783424023357

- *Name:* Tornado.Cash: L1 Helper
- *Description:* Allows users to designate deposited Ether to be bridged to a Tornado Cash pool located on the Gnosis Chain blockchain. This smart contract is not a major component of the Tornado Cash application.
- *Still in use:* Yes.
- *Governance Controls:* No significant controls. The community may choose to withdraw tokens sent to this contract, as it is not an intended recipient.

- 0x722122dF12D4e14e13Ac3b6895a86e84145b6967
  - *Name:* Tornado.Cash: Proxy
  - *Description:* An old version of *Tornado.Cash: Router*.
  - *Still in use:* No, this is associated with an older version of Tornado Cash.
  - *Governance Controls:* No significant controls following deprecation of this contract in Feb 2022. The community may choose to withdraw tokens sent to this contract, as it is not an intended recipient.
- 0x905b63Fff465B9fFBF41DeA908CEb12478ec7601
  - *Name:* Tornado.Cash: Old Proxy
  - *Description:* An old version of *Tornado.Cash: Router*.
  - *Still in use:* No, this is associated with an older version of Tornado Cash.
  - *Governance Controls:* No significant controls. The community may choose to withdraw tokens sent to this contract, as it is not an intended recipient.

C: List of outdated contracts that retain an operator permission

- 0x94A1B5CdB22c43faab4AbEb5c74999895464Ddaf
  - *Name:* Tornado.Cash: Mixer 1
  - *Description:* An old version of the Tornado Cash pools, unused today.
  - *Operator:* 0x8589427373D6D84E98730D7795D8f6f8731FDA16, aka *Tornado Cash: Donate*
  - *Operator Controls:*
    - This contract cannot be removed by anyone.
    - The sole permission afforded to the Operator is the permission to "enable" and "disable" the use of the contract. As of Oct 2019, the operator has "disabled" use of the contract.
- 0xb541fc07bC7619fD4062A54d96268525cBC6FfEF
  - *Name:* Tornado.Cash: Mixer 2
  - *Description:* An old version of the Tornado Cash pools, unused today.
  - *Operator:* 0xDD4c48C0B24039969fC16D1cdF626eaB821d3384, aka *Gitcoin Grants: Tornado.cash*
  - *Operator Controls:* Updatable by the operator.
- 0xF60dD140cFf0706bAE9Cd734Ac3ae76AD9eBC32A
  - *Name:* Tornado.Cash: 10000 DAI
  - *Description:* Old/unused Tornado Cash pool that allows deposits and withdrawals in increments of 10000 DAI.
  - *Last used:* Feb, 2020

- *Operator:* 0xDD4c48C0B24039969fC16D1cdF626eaB821d3384, aka *Gitcoin Grants: Tornado.cash*
- *Operator Controls:*
  - This contract cannot be removed by anyone.
  - The sole permission afforded to the Operator is the permission to update the "verifier" used by the contract. In essence, the Operator may change how this contract processes zero-knowledge proofs.

- 0xb1C8094B234DcE6e03f10a5b673c1d8C69739A00
  - *Name:* Tornado.Cash: 500000 cDAI
  - *Description:* Unused Tornado Cash pool that allows deposits and withdrawals in increments of 500000 cDAI.
  - *Last used:* Never used
  - *Operator:* 0xDD4c48C0B24039969fC16D1cdF626eaB821d3384, aka *Gitcoin Grants: Tornado.cash*
  - *Operator Controls:*
    - This contract cannot be removed by anyone.
    - The sole permission afforded to the Operator is the permission to update the "verifier" used by the contract. In essence, the Operator may change how this contract processes zero-knowledge proofs.

- 0xD691F27f38B395864Ea86CfC7253969B409c362d
  - *Name:* Tornado.Cash: 10000 USDC
  - *Description:* Unused Tornado Cash pool that allows deposits and withdrawals in increments of 10000 USDC.

- *Last used:* Never used
- *Operator:* 0xDD4c48C0B24039969fC16D1cdF626eaB821d3384, aka *Gitcoin Grants: Tornado.cash*
- *Operator Controls:*
  - This contract cannot be removed by anyone.
  - The sole permission afforded to the Operator is the permission to update the "verifier" used by the contract. In essence, the Operator may change how this contract processes zero-knowledge proofs.

- 0xaEaaC358560e11f52454D997AAFF2c5731B6f8a6
  - *Name:* Tornado.Cash: 5000 cUSDC
  - *Description:* Old/unused Tornado Cash pool that allows deposits and withdrawals in increments of 5000 cUSDC.
  - *Last used:* May, 2020
  - *Operator:* 0xDD4c48C0B24039969fC16D1cdF626eaB821d3384, aka *Gitcoin Grants: Tornado.cash*
  - *Operator Controls:*
    - This contract cannot be removed by anyone.
    - The sole permission afforded to the Operator is the permission to update the "verifier" used by the contract. In essence, the Operator may change how this contract processes zero-knowledge proofs.
- 0x1356c899D8C9467C7f71C195612F8A395aBf2f0a
  - *Name:* Tornado.Cash: 50000 cUSDC

- *Description:* Unused Tornado Cash pool that allows deposits and withdrawals in increments of 50000 cUSDC.
- *Last used:* Never used
- *Operator:* 0xDD4c48C0B24039969fC16D1cdF626eaB821d3384, aka *Gitcoin Grants: Tornado.cash*
- *Operator Controls:*
  - This contract cannot be removed by anyone.
  - The sole permission afforded to the Operator is the permission to update the "verifier" used by the contract. In essence, the Operator may change how this contract processes zero-knowledge proofs.

- 0xA60C772958a3eD56c1F15dD055bA37AC8e523a0D
  - *Name:* Tornado.Cash: 500000 cUSDC
  - *Description:* Unused Tornado Cash pool that allows deposits and withdrawals in increments of 500000 cUSDC.
  - *Last used:* Never used
  - *Operator:* 0xDD4c48C0B24039969fC16D1cdF626eaB821d3384, aka *Gitcoin Grants: Tornado.cash*
  - *Operator Controls:*
    - This contract cannot be removed by anyone.
    - The sole permission afforded to the Operator is the permission to update the "verifier" used by the contract. In essence, the Operator may change how this contract processes zero-knowledge proofs.

- 0xF67721A2D8F736E75a49FdD7FAd2e31D8676542a
  - *Name:* Tornado.Cash: 10000 USDT
  - *Description:* Old/unused Tornado Cash pool that allows deposits and withdrawals in increments of 10000 USDT.
  - *Last used:* May, 2020
  - *Operator:* 0xDD4c48C0B24039969fC16D1cdF626eaB821d3384, aka *Gitcoin Grants: Tornado.cash*
  - *Operator Controls:*
    - This contract cannot be removed by anyone.
    - The sole permission afforded to the Operator is the permission to update the "verifier" used by the contract. In essence, the Operator may change how this contract processes zero-knowledge proofs.
- 0x9AD122c22B14202B4490eDAf288FDb3C7cb3ff5E
  - *Name:* Tornado.Cash: 100000 USDT
  - *Description:* Unused Tornado Cash pool that allows deposits and withdrawals in increments of 100000 USDT.
  - *Last used:* Never used
  - *Operator:* 0xDD4c48C0B24039969fC16D1cdF626eaB821d3384, aka *Gitcoin Grants: Tornado.cash*
  - *Operator Controls:*
    - This contract cannot be removed by anyone.
    - The sole permission afforded to the Operator is the permission to update the "verifier" used by the

contract. In essence, the Operator may change how this contract processes zero-knowledge proofs.

D: List of donation addresses

- 0xDD4c48C0B24039969fC16D1cdF626eaB821d3384
  - *Name:* Gitcoin Grants: Tornado.cash
  - *Description:* A smart contract used to receive software development grants from the Gitcoin crowdfunding platform.
- 0x8589427373D6D84E98730D7795D8f6f8731FDA16
  - *Name:* Tornado.Cash: Donate
  - *Description:* A user address used to receive donations for software development. This address is not a smart contract.

Acknowledgements

- Shayan Eskandari (@sbetamc)
- Mikerah (@badcryptobitch)
- Banteg (@bantg)
- Wavey (@wavey0x)
- Hudson Jameson (@hudsonjameson)
- Kirill Pimenov (@kirushik)

- Mike Wawszczak (@mikedotwaves)
- Mary Mallor (@mmaller)
- M (@PopcornandWhiskey)
- Milo Murphy

Thank you to these independent researchers and advocates who donated their time and expertise to this effort.

Coin Center

Washington, DC

info@coincenter.org

@coincenter

Sitemap

Coin Center Policy Briefing

Receive periodic updates on policy research, testimony, and other Coin Center news.

Type your e | Subscribe

substack

EXHIBIT 63

Crypto Mixers and AML Compliance

blog.chainalysis.com/reports/crypto-mixers/

Chainalysis Team

August 23, 2022

What is a crypto mixer?

A crypto mixer is a service that blends the cryptocurrencies of many users together to obfuscate the origins and owners of the funds. Because Bitcoin, Ethereum, and most other public blockchains are transparent, this level of privacy is otherwise hard to achieve.

Why are crypto mixers used?

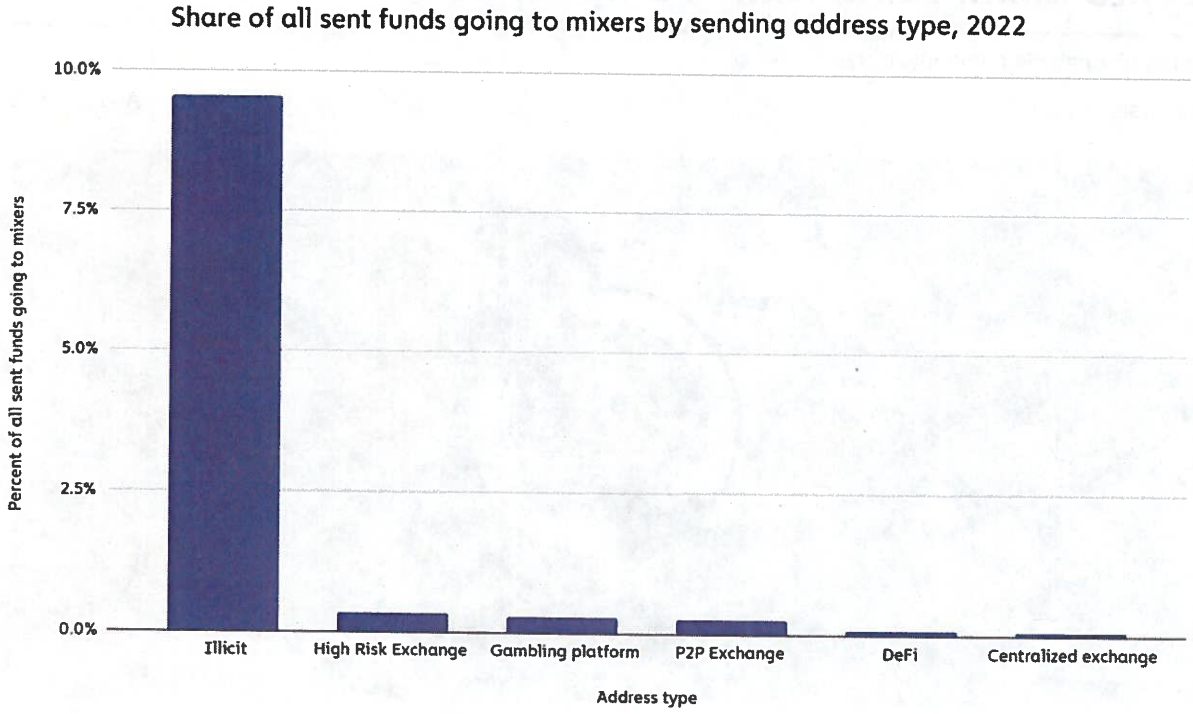
Financial privacy

Many use mixers out of a preference or need for privacy. Financial privacy is important, especially to those who live under oppressive regimes or who wish to make legal transactions anonymously.

Money laundering

A small percentage of crypto mixer users are cybercriminals. These criminals use mixers to obscure the connection between the crypto wallets they use to collect their illicit profits and the crypto wallets from which they transfer their funds to crypto-to-fiat exchanges. In this way, they aim to avoid triggering anti-money laundering alerts.

In July, we found that almost 10% of all cryptocurrencies held by illicit entities have been laundered through a mixer in 2022.



By comparison, only 0.3% of cryptocurrencies exposed to gray-area entities like gambling sites and high-risk exchanges have been mixed. This statistic falls to just 0.1% for cryptocurrencies exposed to regulated entities like centralized exchanges.

How crypto mixers work

Mixers collect, pool and pseudo-randomly shuffle the cryptocurrencies deposited by many users. Later, the funds are withdrawn to new addresses under the control of each user, minus a small service fee.

Most mixers make the deposited funds more difficult to track by letting users schedule their withdrawals in randomized amounts at randomized intervals. Others try to obfuscate the fact that a mixer is even being used; they typically do so by varying the transaction fee and the withdrawal address type.

The different types of crypto mixers

Most mixers fall under one of the following three categories, with the latter categories being the most novel and autonomous.

Centralized custodial mixers

Centralized custodial mixers, which emerged as early as 2011, temporarily take ownership of users' funds and are typically run by a single operator. Because this type of mixing service is both centralized and custodial, users face additional privacy risks. They are also often a target of law enforcement, as financial enforcement agencies treat them as unregistered money services businesses.

CoinJoins

A CoinJoin is a type of mixer commonly built into privacy wallets — meaning cryptocurrency wallets that pitch themselves on increased privacy — that combine users' coins with the coins of multiple other users in a single transaction. Users often repeat this process multiple times.

Unlike centralized mixers, CoinJoins are non-custodial, meaning they never actually hold users' funds.

Smart contract mixers

Like CoinJoins, smart contract mixers are non-custodial. But unlike CoinJoins, smart contract mixers don't combine users' funds in just one transaction. Instead, the user sends their funds to the mixer, receives a cryptographic note proving that they are the depositor, and then, whenever they'd like, sends the mixer that note to withdraw the funds to a new address. In the meantime, the cryptocurrencies are tumbled in a number of different ways.

Smart contract mixers often work with service providers called relayers, which can provide the ether necessary to pay the gas fees on mixer withdrawal transactions. This ensures that the user can withdraw their funds to new addresses with no transaction histories or connections to other services.

Are crypto mixers legal?

Despite their use by criminals, crypto mixers are not explicitly illegal in most jurisdictions. Whether they are compliant, however, is a different question.

In the United States, the Financial Crimes Enforcement Network (FinCEN) has confirmed that individuals and centralized businesses offering custodial mixing services must register as money transmitters under the Bank Secrecy Act (BSA), and have three key obligations:

1. register with FinCEN,
2. maintain an anti-money laundering and know-your-customer compliance program, and
3. meet all applicable reporting and record-keeping requirements.

We aren't aware of any custodial mixers currently following these rules. And given that privacy preservation is the main reason that many users interact with crypto mixers, it seems unlikely that one could implement these procedures and still retain their users.

Sanctions also matter for mixers. All mixers that want to do business in the U.S. must take measures to ensure they don't do business with sanctioned entities. And, as we'll cover below, even non-custodial smart contract-based mixers not covered by the BSA can be subject to sanctions designations, provided of course they aren't based in the U.S.

Enforcement actions against crypto mixers

Server seizures

In May 2019, the Dutch Fiscal Information and Investigation Service (FIOD), in close cooperation with Europol and authorities in Luxembourg, seized six servers controlled by the Bitcoin, Bitcoin Cash and Litecoin mixer Bestmixer.io.

Criminal charges

In April 2021, the Department of Justice (DOJ) arrested and charged the operator of Bitcoin Fog with money laundering, operating an unlicensed money transmitting business, and money transmission without a license.

In August 2021, the operator of the Bitcoin mixer Helix pleaded guilty to money laundering conspiracy and agreed to the forfeiture of more than 4,400 bitcoin, valued at more than $200 million at the time.

Sanctions designations

In May 2022, the U.S. Treasury's Office of Foreign Assets Control (OFAC) issued its first-ever sanctions on a crypto mixer, Blender.io, for its role in laundering funds stolen by North Korea in the hack of Ronin Bridge, a DeFi protocol linked to Axie Infinity.

In August 2022, OFAC sanctioned the most popular Ethereum mixer, Tornado Cash, for its role in laundering funds stolen by North Korean-linked hackers in the attacks on the Ronin and Harmony bridges.

Civil penalties

In October 2020, FinCEN penalized the operator of the Bitcoin mixers Helix and Coin Ninja $60 million dollar civil money penalty for operating two unregistered money services businesses (MSB).

How Chainalysis can help

Our blockchain forensics product, Chainalysis Reactor, has the most extensive mixer coverage and analytics tooling in the industry. Financial privacy is valuable, but so is consumer safety: our data shows that some 25% of mixed funds come from illicit addresses, and cybercriminals associated with hostile governments have mixed some of the largest sums. It's therefore important that stakeholders in the public and private sectors work together to address these risks – and use best-in-class data to inform their decisions.

To that end, Chainalysis's cryptocurrency compliance software, blockchain forensics tools, and government solutions teams are ready to help.

This material is for informational purposes only, and is not intended to provide legal, tax, financial, or investment advice. Recipients should consult their own advisors before making these types of decisions. Chainalysis has no responsibility or liability for any decision made or any other acts or omissions in connection with Recipient's use of this material.

EXHIBIT 87

Decentralizing TornadoCash: The Launch of Tornado Fund and the Path Towards TornadoDAO

medium.com/@Tornado_Fund/decentralizing-tornadocash-the-launch-of-tornado-fund-and-the-path-towards-tornadodao-a6d4ffc6c800

Tornado.Fund July 1, 2020

Tornado.Fund

Jun 29, 2020

5 min read

Today we are announcing the launch of Tornado Fund, a DAO to invest in Tornado Cash and help it develop into the first, fully decentralized privacy-preserving technology for Ethereum.

With the rise of the internet, information and financial transactions are becoming increasingly connected — this data is often cataloged, duplicated, shared, and sold, maintaining our expected levels of privacy can be a challenge. Many of us see the value of having private financial transactions on-chain. At a high-level, privacy enables us to create boundaries and protect ourselves from unwarranted interference in our lives, allowing us to negotiate who we are and how we want to interact with those around us.

Financial freedom — transacting with the need of a middle party — is tied to financial privacy. Outside of the moral justification, our financial privacy is critical for practical reasons as well. We want our transactions to not be viewable to possible criminal third parties, better positions for companies and private individuals that may be in negotiations, contamination that could lead to blacklists, and lastly, but also very importantly, protecting ourselves from financial censorship and prohibition.

Blockchain has some fundamental privacy problems by virtue of the design. On Ethereum, and other blockchains that are publicly available, every transaction can be traced back on a blockchain to the first genesis block. Bitcoin and Ethereum are colloquially known to be "pseudonymous," which means that the transaction addresses, or data points, are not directly associated with a specific individual, however where multiple points can be linked. This results in the transactions and funds being publicly viewable on block explorers, like Etherscan, enabling anyone to uncover your assets, view your payments, trace the source of your funds, calculate your holdings, and analyze your on-chain activity.

Over the years there have been attempts to create private transactions on Ethereum. For example, users have tried to maintain their financial privacy by obscuring value flows through a centralized exchange. Others restored to using custodial mixing services that created regulatory concerns and risks. These techniques, however, never achieved full privacy due to security concerns or, in the case of a centralized exchange, the disclosure of personally identifiable information.

Tornado Cash addresses these critical blind spots. Tornado Cash is a privacy-preserving technology that uses zero-knowledge proofs which completely breaks the link between the sender and recipient. Unlike other privacy-preserving technologies which "spam" additional transactions in between sender and receiver, Tornado Cash puts user funds within a smart contract in a black-box environment, which isn't visible on-chain. Moreover, Tornado Cash is a decentralized service — run by a smart contract with no centralized third party taking custody or control of funds during the process.

Of equal importance, Tornado Cash has implemented compliance tools that enable users of Tornado Cash to prove the source of their funds (if the need arises). That means that individuals can prove legitimate, lawful uses of Tornado Cash, if requested by regulators.

Not surprisingly, Tornado Cash has generated a tremendous amount of support in the Ethereum ecosystem from members that value and deem privacy essential to scale the technology is a credible, safe, and lawful way. In early May, Tornado Cash conducted a cryptographic process where over 1,100 participants contributed to the largest Trusted Ceremony Setup to date.

Tornado Cash can fully bring to life this vision of financial freedom, privacy included.

Introducing Tornado Fund

The Trusted Ceremony was the first step in making the Tornado Cash protocol trustless, decentralized, and unstoppable. While much of the protocol has been successfully decentralized (including the UX), there is still more to do for the privacy-preserving technology. In order to push this vision forward, the Tornado Cash team, in conjunction with OpenLaw (the project behind The LAO), is creating Tornado Fund, which will be launched in mid-July.

The Tornado Fund is just the first phase in Tornado Cash's evolution towards a fully decentralized protocol. The Tornado Fund will be used specifically to fund the software developers behind Tornado Cash (PepperSec, Inc.) so that they can develop version 3 of the Tornado Cash Protocol. Funding will be used to pay for software development and other operational costs.

The fruits of this effort will be the launch of version 3 of Tornado Cash. Tornado Cash currently does not have a token, and Version 3 may introduce (although there are no guarantees) a protocol level token to govern aspects of the Tornado Cash network.

If Version 3 of Tornado Cash includes a token, its will be accompanied by the creation of a community-owned and operated TornadoDAO — an evolution of the TornadoFund — which will serve a locus for Tornado Cash governance, potentially hold ether, and continue to direct the future of the Tornado Cash protocol.

Under this scenario, the Tornado Fund (a proto-DAO) will evolve into a fully decentralized DAO that helps ensure that protocol developers and other early supporters of the protocol can continue to fuel network development without centralized control. The entire network and protocol will be decentralized and entirely community-driven. The future of Tornado Cash will be in the Ethereum community's hands.

The Structure of Tornado Fund

The Tornado Fund will be organized as a limited liability legal entity in Delaware (Tornado DAO, LLC), using the Moloch v2 smart contracts to handle mechanics related to pooling and deployment of an investment in the Tornado Cash team. All of the relevant legal documents

from the entity formation documents to member subscription agreements will be generated automatically at contribution. In order to comply with United States law, membership interests of the Tornado Fund will be limited and only available to parties that meet the definition of an accredited investor. OpenLaw will serve as the service provider to the DAO and perform the accreditation checks, legal paperwork, servicing the DApp, etc.

Prospective members can purchase units in Tornado Fund (1% interest) in exchange for 30 eth. There will be up to 100 members of Tornado Fund making the total amount collected in Tornado Fund 3,000 eth (or about $700,000 USD). All proceeds raised by the Tornado Fund will be used to fund the Tornado Cash team and the investment will be structured as a convertible note, with a right to receive a proportional amount of any tokens reserved by the Tornado Cash team, if the member of TornadoDAO determine that those tokens are not securities.

Joining the Tornado Fund

If you're interested in becoming a member of the Tornado Fund, you can pre-register here. This will give you a leg up when the Fund launches in mid-July.

(Note: OpenLaw's role in the creation and maintenance of the Tornado Fund will be that of an administrator. OpenLaw will exercise no control over Tornado Fund, unless directed by the members. For these services, OpenLaw will receive a fee for its role in creating and maintaining the software necessary. The fee will be used to pay for ongoing software development and other costs necessary to set up and maintain the OpenLaw protocol. The Tornado Fund is a proto-DAO and will have no general partner.)

Learn More

To learn more about Tornado Fund, sign-up and continue the conversation on our Telegram and follow us on our Twitter. If you'd like to check out our documentation and FAQs, please do so here. Reach out with any questions at hello@tornadofund.io. We look forward to having you join the community!

EXHIBIT 89

ALL ARTICLES > UNIVERSITY

Crypto Tokens vs Coins — What's the Difference?

Are crypto tokens and coins the same thing? Not exactly. Here we explain how to tell a coin from a token, and their different uses.

JUN 20, 2022 | BEGINNER

Key Takeaways

Coins

- A crypto coin is a form of digital currency that's often native to its blockchain; it stores value and acts as a medium of exchange

- Coins can be mined through proof of work (PoW) or earned through proof of stake (PoS)
- Examples include Bitcoin (BTC), Ether (ETH), and Cardano (ADA)

Tokens

- A crypto token is built for a decentralised project on an existing blockchain (usually Ethereum, the most popular blockchain for decentralised projects to build upon)
- A token represents an asset or offers holders certain platform-specific features
- Tokens offer functions, including utility, security, and governance
- Examples include Cronos (CRO), Very, Very Simple Finance (VVS), and Uniswap (UNI)

Token vs Coin: What is the Difference?

While many people use the phrases 'crypto coin', 'crypto token', and 'cryptocurrency' interchangeably, they're not the same thing. Though coins and tokens use distributed ledger technology (also known as blockchain technology), there are some significant differences between a coin and a token.

The TLDR is: Crypto coins are a form of digital currency that are often native to a blockchain, with the main purpose of storing value and working as a medium of exchange.

Crypto tokens are digital assets that are built on top of an existing blockchain (using smart contracts) and can serve a wide variety of functions, from representing a physical object to granting access to platform-specific services and features.

What is a Crypto Coin?

Crypto coins are native to their own blockchain. The Bitcoin blockchain coin is BTC. The Ethereum blockchain has ETH. And the Litecoin blockchain uses LTC. These crypto coins are primarily designed to store value and work as a medium of exchange, similar to traditional currencies. This is why crypto coins are also referred to as cryptocurrencies.

One of the other unique things about coins is the way they come into being. Generally, crypto coins are either mined using a proof of work (PoW) consensus mechanism or earned via a proof of stake (PoS) mechanism.

What are Coins Used for?

When Bitcoin was created, it was envisioned as a replacement for traditional fiat currencies.

Along with other crypto coins, it was **designed to work in the same ways as paper money** and metal coins, meaning it can be used for many of the things normally used with US dollars or Euros, including:

- Storing value
- Exchanging for other currencies
- Paying for goods and services
- Transferring to others

In addition to these traditional uses, some crypto coins can also take advantage of smart contract technology to offer additional features. For example, DASH is an altcoin that acts as a cryptocurrency but also gives holders the ability to vote in a decentralised autonomous organisation (DAO).

Popular Crypto Coins

- **Bitcoin (BTC)** was launched in early 2009 by the mysterious 'Satoshi Nakamoto', Bitcoin is the first and most well-known crypto coin in the world. Its head start has allowed it to become the most valuable cryptocurrency
- **Ether (ETH)** is one of the most popular crypto coins around and more than just a cryptocurrency. Thanks to the creation and implementation of smart contracts, Ethereum has become home to thousands of blockchain projects and NFTs. In some ways, it's the backbone of the blockchain revolution
- **Cardano (ADA)** is an open-source and decentralised blockchain platform that was one of the first to run on a PoS consensus, gaining a rep as a green crypto coin. Cardano was founded in 2015 by Ethereum co-founder Charles Hoskinson and facilitates peer-to-peer (P2P) transactions with its coin ADA

What are Tokens?

Like crypto coins, crypto tokens are designed using blockchain technology; however, crypto tokens aren't native to a blockchain. Instead, they're built on top of it, often utilising smart contracts to fulfil a variety of purposes.

While crypto coins mimic traditional currencies, crypto tokens are more like assets or even deeds. A crypto token can represent a share of ownership in a DAO, a digital product or NFT, or even a physical object. Crypto tokens can be bought, sold, and traded like coins, but they aren't used as a medium of exchange.

To use a real-world example, crypto tokens are more like coupons or vouchers, while crypto coins are like dollars and cents.

There are numerous types of crypto tokens:

Some governance tokens offer holders voting rights in a DAO.

Utility tokens may provide access to certain services or products developed by the token issuer.

Security tokens act like traditional securities and are even treated the same by many governmental agencies.

What are Tokens Used for?

Most crypto tokens are designed to be used within a blockchain project or dapp. Unlike crypto coins, tokens aren't mined; they are created and distributed by the project developer. Once tokens are in the hands of purchasers, they can be used in countless ways.

Popular Crypto Tokens

- **Filecoin** (FIL) and **Arweave** (AR) give users the ability to spend their utility tokens for the privilege of storing data on their decentralised network, pushing the concept of cloud storage to its full potential

- **Axie Infinity,** one of the best-known play-to-earn (P2E) on the market, features a utility token called **Smooth Love Potions** (SLP). By earning or purchasing SLP, players can perform exclusive in-game tasks

- **Cronos** (CRO) is the utility token for the Crypto.com ecosystem. CRO can be used to pay fees on the platform or staked for various benefits, and it allows token holders to trade crypto tokens for fiat at a reduced price

What About Stablecoins? Are They Coins or Tokens?

Stablecoins are cryptocurrencies tied to specific assets. They are a bit of a misnomer, as most of them are actually ERC-20 tokens (i.e., they operate on the Ethereum blockchain through a smart contract). So why are they called stable*coins*? The name lends itself to their primary function of being a medium of exchange.

Take **USD Coin (USDC),** for example. It is a smart-contract-based stablecoin (i.e., it doesn't have its own chain and is an ERC-20 token). It is backed by US dollars, held by the company that issues the token, to maintain the value of every USDC at US$1.

Conclusion

The question of whether to buy coins or tokens is largely dependent upon a holder's goals. Both can be purchased in the Crypto.com App or on the Crypto.com Exchange with low fees and best execution prices.

Browse our data and descriptions of thousands of coins and tokens on Crypto.com Price.

Due Diligence and Do Your Own Research

All examples listed in this article are for informational purposes only. You should not construe any such information or other material as legal, tax, investment, financial, or other advice. Nothing contained herein shall constitute a solicitation, recommendation, endorsement, or offer by Crypto.com to invest, buy, or sell any coins, tokens, or other crypto assets. Returns on the buying and selling of crypto assets may be subject to tax, including capital gains tax, in your jurisdiction.

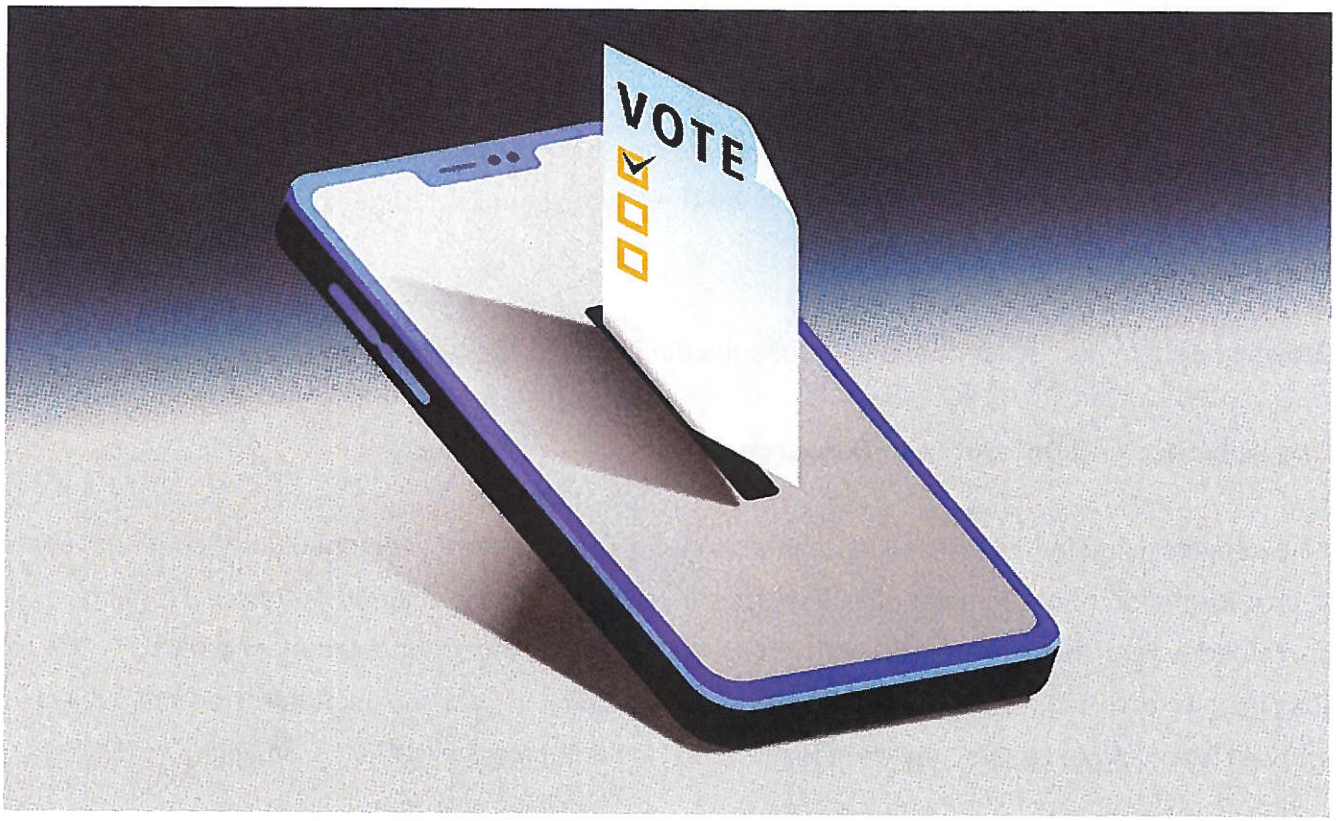
Past performance is not a guarantee or predictor of future performance. The value of crypto assets can increase or decrease, and you could lose all or a substantial amount of your purchase price. When assessing a crypto asset, it's essential for you to do your research and due diligence to make the best possible judgement, as any purchases shall be your sole responsibility.

Tags

ALTCOINS / COINS / COINS & TOKENS / CRYPTO101 / CRYPTOCURRENCIES / TOKENS

Share with Friends

RELATED CONTENT

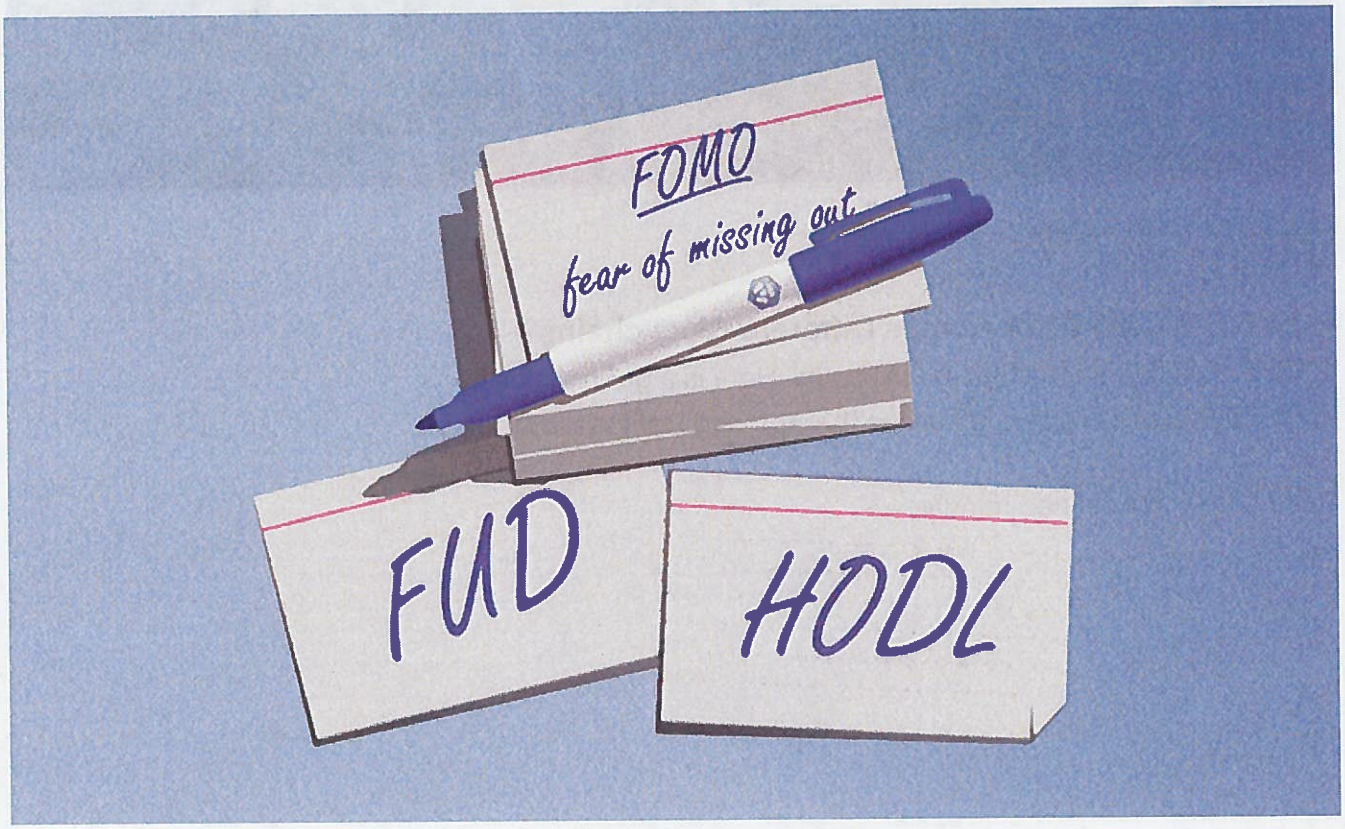


UNIVERSITY / COINS & TOKENS
JUL 11, 2022

What Are Governance Tokens?

Governance tokens give holders a voice in crypto and blockchain projects. Learn how it works in detail.

Read More - (undefined minute)



UNIVERSITY / COINS & TOKENS
AUG 31, 2022

Crypto Slang: 28 Terms You Should Know

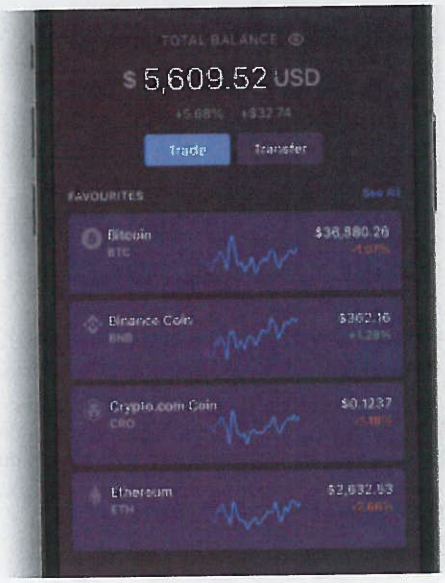
The crypto world is full of technical jargon, slang, and acronyms. Here's everything to know so you can join the conversation.

Read More - (undefined minute)

UNIVERSITY / COINS & TOKENS
SEP 20, 2022

How Does CRO Work Across Different Blockchains?
CRO is available on multiple blockchains. Here is a guide on using and bridging the different tokens in the App and DeFi Wallet.

Read More - (undefined minute)



App

Cards

Commerce

Blockchain

DeFi

Resources

Learn

Company

NFT NEW

EXHIBIT 90

Token TORN Token

Tornado.Cash

Overview [ERC-20]

PRICE	FULLY DILUTED MARKET CAP
$6.37 @ 0.004818 Eth (-1.77%)	$63,699,984.25

Max Total Supply:	9,999,997.52681499910... TORN
Holders:	8,164 (▲ 0.196%)
Transfers:	208,866

Profile Summary [Edit]

Contract:	0x77777feddddffc19ff86db637967013e6c6...
Decimals:	18
Official Site:	https://tornado.cash/
Social Profiles:	

Transfers | Holders | Info | DEX Trades | Contract | Analytics | Comments

Top 1,000 holders (From a total of 8,164 holders)

First < Page 1 of 20 >

Rank	Address	Quantity	Percentage	Value	An
1	Tornado.Cash: Governance Vesting	4,125,000	41.2500%	$26,317,500.00	
2	Binance 8	1,809,480	18.0948%	$11,544,482.40	
3	Tornado.Cash: Governance	1,257,991.900828287048866151	12.5799%	$8,025,988.33	
4	Tornado.Cash: Governance Vault	504,436.363512253822084948	5.0444%	$3,218,304.00	
5	Tornado.Cash: Team 2 Vesting	388,358.861111111111111112	3.8836%	$2,477,729.53	
6	Tornado.Cash: Team 1 Vesting	342,669.583333333333333334	3.4267%	$2,186,231.94	
7	Tornado.Cash: Team 3 Vesting	342,669.583333333333333334	3.4267%	$2,186,231.94	
8	Tornado.Cash: Team 4 Vesting	236,111.111111111111111112	2.3611%	$1,506,388.89	
9	Tornado.Cash: Governance Staking	125,787.300002635135738651	1.2579%	$802,522.97	
10	OKEx	102,084.931162241284050797	1.0208%	$651,301.86	
11	Binance 14	87,756.677098993650782111	0.8776%	$559,887.60	
12	Sablier v1.1	65,299.9999999999817664	0.6530%	$416,614.00	
13	Tornado.Cash: Team 5 Vesting	32,779	0.3278%	$209,130.02	
14	0xd2800879f604cd13d7d9e8738c080408d7105c60	22,550.055302732940298889	0.2255%	$143,869.35	
15	0x5e8304b5600cccba6d6292c6687ac9ead0ec6288	18,744.706	0.1874%	$119,591.22	
16	0			2	
17	0xf1198d0437bcabbb12b8f30ac0e598fd42f89e88	16 254.387797275693083797	0.1625%	$103,702.99	

18	Binance 16	15,115.61730849	0.1512%	$96,437.64
19	0xe0ab8aa177c593bd131c462802a3f29909d6da73	14,285.715	0.1429%	$91,142.86
20	0x2c92193e5f84d19ffcb20d58e58cf230b7c92bf3	13,616.39207	0.1362%	$86,872.58
21	Binance 15	13,293.15796848	0.1329%	$84,810.35
22	Uniswap V3: TORN 2	12,821.64740551634707627	0.1282%	$81,802.11
23	Gate.io	11,924.051032907346327157	0.1192%	$76,075.45
24	0x2a49781a61d9f2d0982053091184e8dd533b7e1a	11,904.7625	0.1190%	$75,952.38
25	Sablier v1.0	10,887.19033009892823667	0.1089%	$69,460.27
26	Uniswap V2: TORN 3	10,370.974018865566109335	0.1037%	$66,166.81
27	0x6d4beb94f60ec025e64a375a7df00980afc34bde	9,999.233	0.1000%	$63,795.11
28	0x6147e468231f2df9fa370d45edddde9010b765cc	9,634.610933058352427605	0.0963%	$61,468.82
29	0x1ef7d375b5325a8aaa3c0dc6667c147f41e63a1d	9,181.642	0.0918%	$58,578.88
30	0xddbc1841be23b2ab55501deb4d6bc39e3f8aa2d7	9,109.08133	0.0911%	$58,115.94
31	0x758ab8ac42a8c44df8c31129db146c65c2669391	7,999.58	0.0800%	$51,037.32
32	Gate.io 3	7,598.243446356703392492	0.0760%	$48,476.79
33	Mexc.com 3	7,326.86356	0.0733%	$46,745.39
34	1inch: ETH-TORN Pool	6,790.55076043925655953	0.0679%	$43,323.71
35	Tornado.Cash: Reward Swap	6,675.064596850152391553	0.0668%	$42,586.91
36	0xa6650193bd0c6979136f54aa5c4ebf915b57b642	6,395.40558	0.0640%	$40,802.69
37	0x8ba2262becc5eaa0d95386f9a0197225367168cf	6,304.163315641904238499	0.0630%	$40,220.56
38	0x7bc0fbabea25c0e6c47f06b0e95b43620ec25c26	5,816.744043639236780714	0.0582%	$37,110.83
39	0x22dd0967542ebdb70fb7232cf0a78f5868a498ce	5,798.167172558087375261	0.0580%	$36,992.31
40	Celer Network: cBridge V2	5,068.508386763187496873	0.0507%	$32,337.08
41	0x5bdf85216ec1e38d6458c870992a69e38e03f7ef	4,992.030910898612	0.0499%	$31,849.16
42	0x2fb386d2de55a443fdc4033e14905ef2f96e1d07	4,761.905	0.0476%	$30,380.95
43	Poloniex 4	4,019.031915623377721111	0.0402%	$25,641.42
44	MEXC: Mexc.com	4,011.220245867596942986	0.0401%	$25,591.59
45	0xd1a8b3ef24154df24d1b4bcf3baacd7fcaabac59	3,350.354930209624140583	0.0335%	$21,375.26
46	0x69383889dbb0b45f83b82aa25b7015cc1bd0ae76	3,211.808057498366549384	0.0321%	$20,491.34
47	0			
48	0			

49	0x3c9ebcf717582c46afc43c700c53e500095af726	3,000	0.0300%	$19,140.00	
50	0xd52cac9b0ff0b1b6236797147405a92491ee062f	2,841.253283347325798419	0.0284%	$18,127.20	

First < Page 1 of 20 >

[Download CSV Export]

A token is a representation of an on-chain or off-chain asset. The token page shows information such as price, total supply, holders, transfers and social links. Learn more about this page in our Knowledge Base.

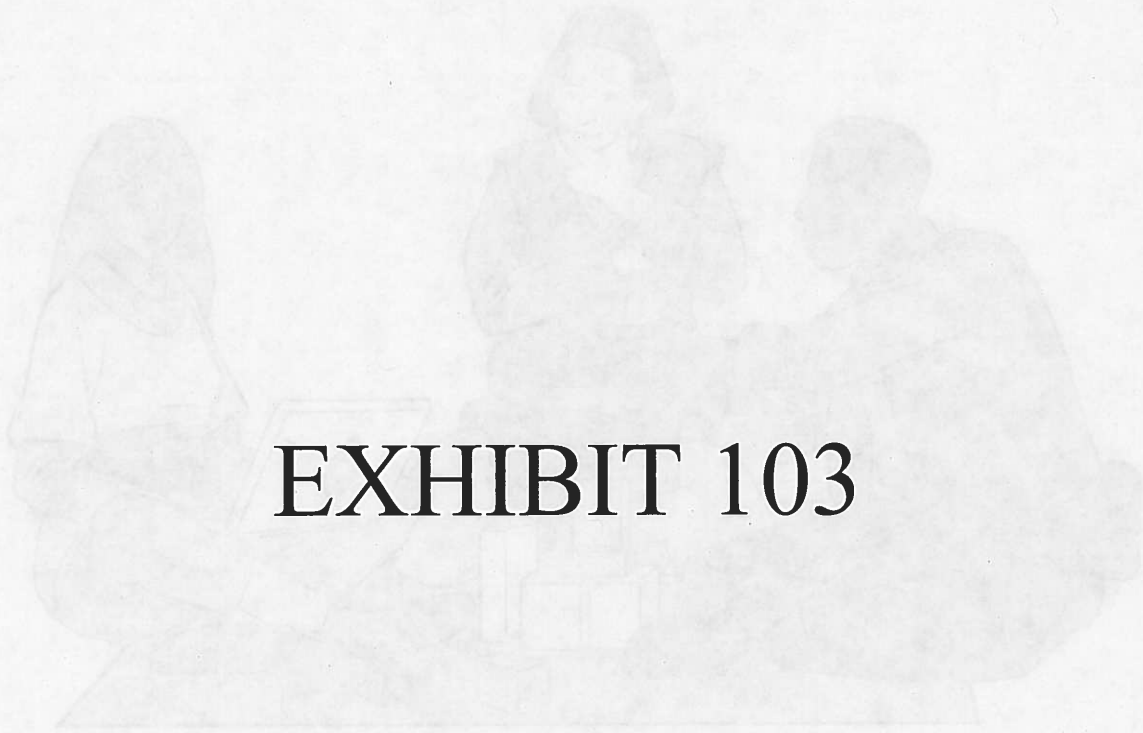
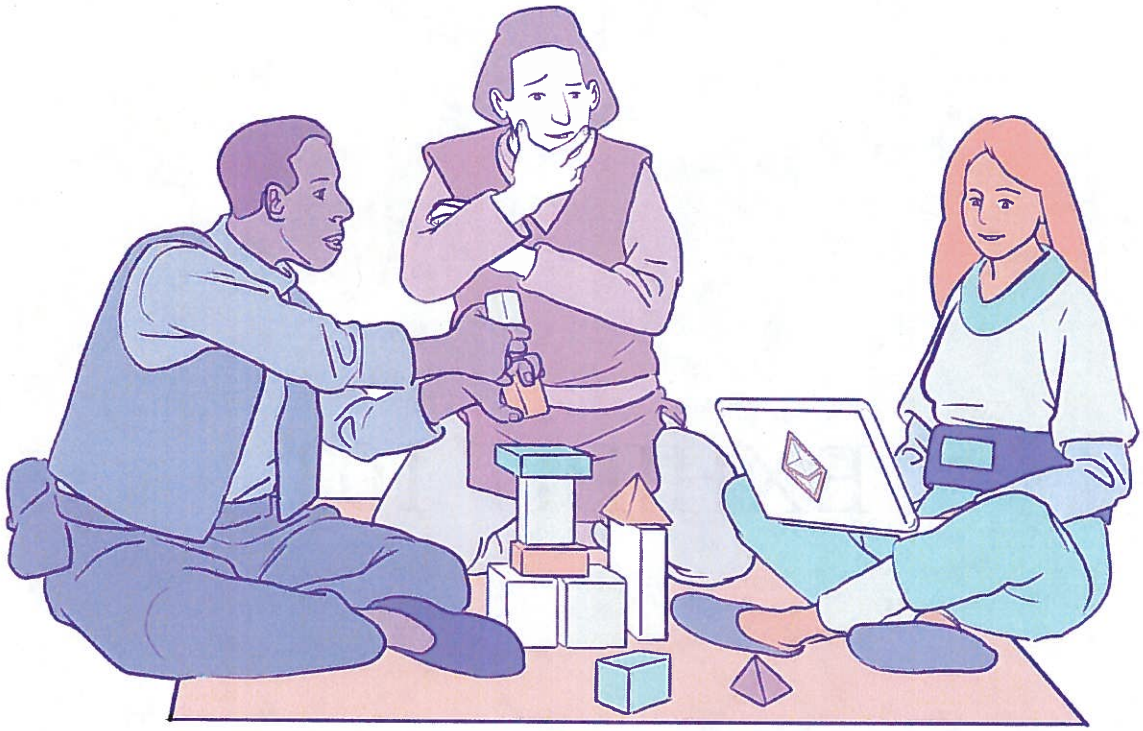


EXHIBIT 103

Intro to Ethereum

ethereum.org/en/developers/docs/intro-to-ethereum/



Last edit: , Invalid DateTime

Edit page

On this page

What is a blockchain?

A blockchain is a public database that is updated and shared across many computers in a network.

"Block" refers to data and state being stored in consecutive groups known as "blocks". If you send ETH to someone else, the transaction data needs to be added to a block to be successful.

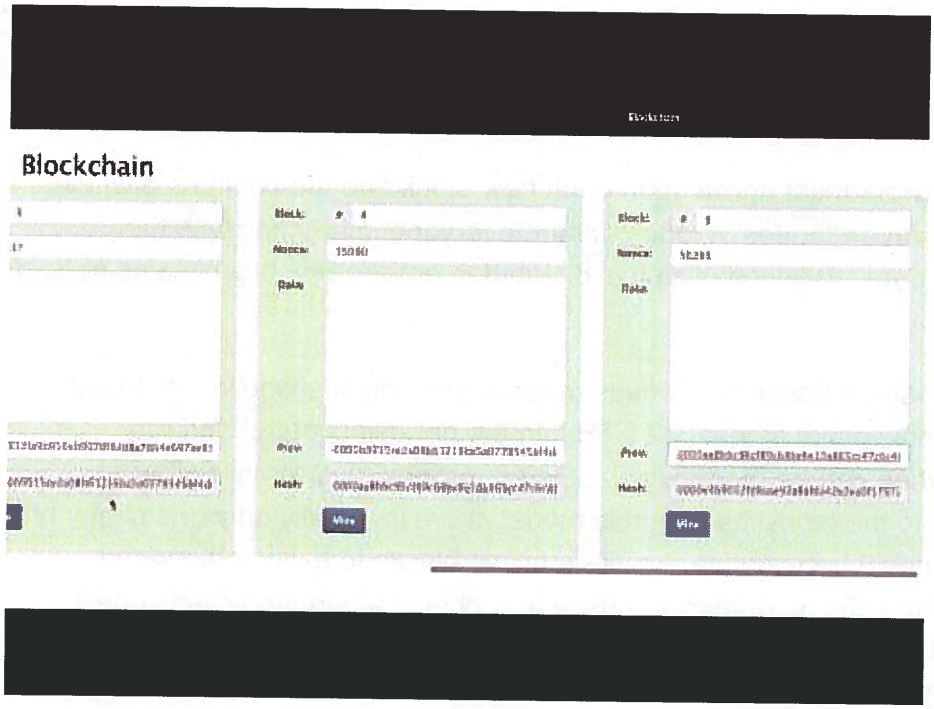
"Chain" refers to the fact that each block cryptographically references its parent. In other words, blocks get chained together. The data in a block cannot change without changing all subsequent blocks, which would require the consensus of the entire network.

Every computer in the network must agree upon each new block and the chain as a whole. These computers are known as "nodes". Nodes ensure everyone interacting with the blockchain has the same data. To accomplish this distributed agreement, blockchains need a consensus mechanism.

Ethereum uses a proof-of-stake-based consensus mechanism. Anyone who wants to add new blocks to the chain must stake at least 32 ETH into the deposit contract and run validator software. They then can be randomly selected to propose blocks that other validators check and add to the blockchain. In this model, there is usually only one chain, but network latency and dishonest behavior can cause multiple blocks to exist at the same position near the head of the chain. To resolve this, a fork-choice algorithm selects one canonical set of blocks. The blocks selected are the ones that form the heaviest possible chain, where 'heavy' refers to the number of validators that have endorsed the blocks (weighted by the ETH they have staked). There is a system of rewards and penalties that strongly incentivize participants to be honest and online as much as possible.

If you want to see how blockchain hashes data and then the previous block references all the past blocks, be sure to check out this demo by Anders Brownworth and watch the accompanying video below.

Watch Anders explain hashes in blockchains:



Watch Video At: https://youtu.be/_160oMzblY8

What is Ethereum?

Ethereum is a blockchain with a computer embedded in it. It is the foundation for building apps and organizations in a decentralized, permissionless, censorship-resistant way.

In the Ethereum universe, there is a single, canonical computer (called the Ethereum Virtual Machine, or EVM) whose state everyone on the Ethereum network agrees on. Everyone who participates in the Ethereum network (every Ethereum node) keeps a copy of the state of this computer. Additionally, any participant can broadcast a request for this computer to perform arbitrary computation. Whenever such a request is broadcast, other participants on the network verify, validate, and carry out ("execute") the computation. This execution causes a state change in the EVM, which is committed and propagated throughout the entire network.

Requests for computation are called transaction requests; the record of all transactions and the EVM's present state gets stored on the blockchain, which in turn is stored and agreed upon by all nodes.

Cryptographic mechanisms ensure that once transactions are verified as valid and added to the blockchain, they can't be tampered with later. The same mechanisms also ensure that all transactions are signed and executed with appropriate "permissions" (no one should be able to send digital assets from Alice's account, except for Alice herself).

What is ether?

Ether (ETH) is the native cryptocurrency of Ethereum. The purpose of ETH is to allow for a market for computation. Such a market provides an economic incentive for participants to verify and execute transaction requests and provide computational resources to the network.

Any participant who broadcasts a transaction request must also offer some amount of ETH to the network as a bounty. The network will award this bounty to whoever eventually does the work of verifying the transaction, executing it, committing it to the blockchain, and broadcasting it to the network.

The amount of ETH paid corresponds to the time required to do the computation. These bounties also prevent malicious participants from intentionally clogging the network by requesting the execution of infinite computation or other resource-intensive scripts, as these participants must pay for computation time.

ETH is also used to provide crypto-economic security to the network in three main ways: 1) it is used as a means to reward validators who propose blocks or call out dishonest behavior by other validators; 2) It is staked by validators, acting as collateral against dishonest behavior—if validators attempt to misbehave their ETH can be destroyed; 3) it is used to weight 'votes' for newly proposed blocks, feeding into the fork-choice part of the consensus mechanism.

What are smart contracts?

In practice, participants don't write new code every time they want to request a computation on the EVM. Rather, application developers upload programs (reusable snippets of code) into EVM state, and users make requests to execute these code snippets with varying parameters. We call the programs uploaded to and executed by the network smart contracts.

At a very basic level, you can think of a smart contract like a sort of vending machine: a script that, when called with certain parameters, performs some actions or computation if certain conditions are satisfied. For example, a simple vendor smart contract could create and assign ownership of a digital asset if the caller sends ETH to a specific recipient.

Any developer can create a smart contract and make it public to the network, using the blockchain as its data layer, for a fee paid to the network. Any user can then call the smart contract to execute its code, again for a fee paid to the network.

Thus, with smart contracts, developers can build and deploy arbitrarily complex user-facing apps and services such as: marketplaces, financial instruments, games, etc.

Terminology

Blockchain

The sequence of all blocks that have been committed to the Ethereum network in the history of the network. So named because each block contains a reference to the previous block, which helps us maintain an ordering over all blocks (and thus over the precise history).

ETH

Ether (ETH) is the native cryptocurrency of Ethereum. Users pay ETH to other users to have their code execution requests fulfilled.

More on ETH

EVM

The Ethereum Virtual Machine is the global virtual computer whose state every participant on the Ethereum network stores and agrees on. Any participant can request the execution of arbitrary code on the EVM; code execution changes the state of the EVM.

More on the EVM

Nodes

The real-life machines which are storing the EVM state. Nodes communicate with each other to propagate information about the EVM state and new state changes. Any user can also request the execution of code by broadcasting a code execution request from a node. The Ethereum network itself is the aggregate of all Ethereum nodes and their communications.

More on nodes

Accounts

Where ETH is stored. Users can initialize accounts, deposit ETH into the accounts, and transfer ETH from their accounts to other users. Accounts and account balances are stored in a big table in the EVM; they are a part of the overall EVM state.

More on accounts

Transactions

A "transaction request" is the formal term for a request for code execution on the EVM, and a "transaction" is a fulfilled transaction request and the associated change in the EVM state. Any user can broadcast a transaction request to the network from a node. For the transaction request to affect the agreed-upon EVM state, it must be validated, executed, and

"committed to the network" by another node. Execution of any code causes a state change in the EVM; upon commitment, this state change is broadcast to all nodes in the network. Some examples of transactions:

- Send X ETH from my account to Alice's account.
- Publish some smart contract code into EVM state.
- Execute the code of the smart contract at address X in the EVM, with arguments Y.

More on transactions

Blocks

The volume of transactions is very high, so transactions are "committed" in batches, or blocks. Blocks generally contain dozens to hundreds of transactions.

More on blocks

Smart contracts

A reusable snippet of code (a program) which a developer publishes into EVM state. Anyone can request that the smart contract code be executed by making a transaction request. Because developers can write arbitrary executable applications into the EVM (games, marketplaces, financial instruments, etc.) by publishing smart contracts, these are often also called dapps, or Decentralized Apps.

More on smart contracts

Further reading

Know of a community resource that helped you? Edit this page and add it!

Related tutorials

A developer's guide to Ethereum, part 1 – *A very beginner-friendly exploration of Ethereum using Python and web3.py*

Back to top ↑

Was this article helpful?

Next

Intro to Ether

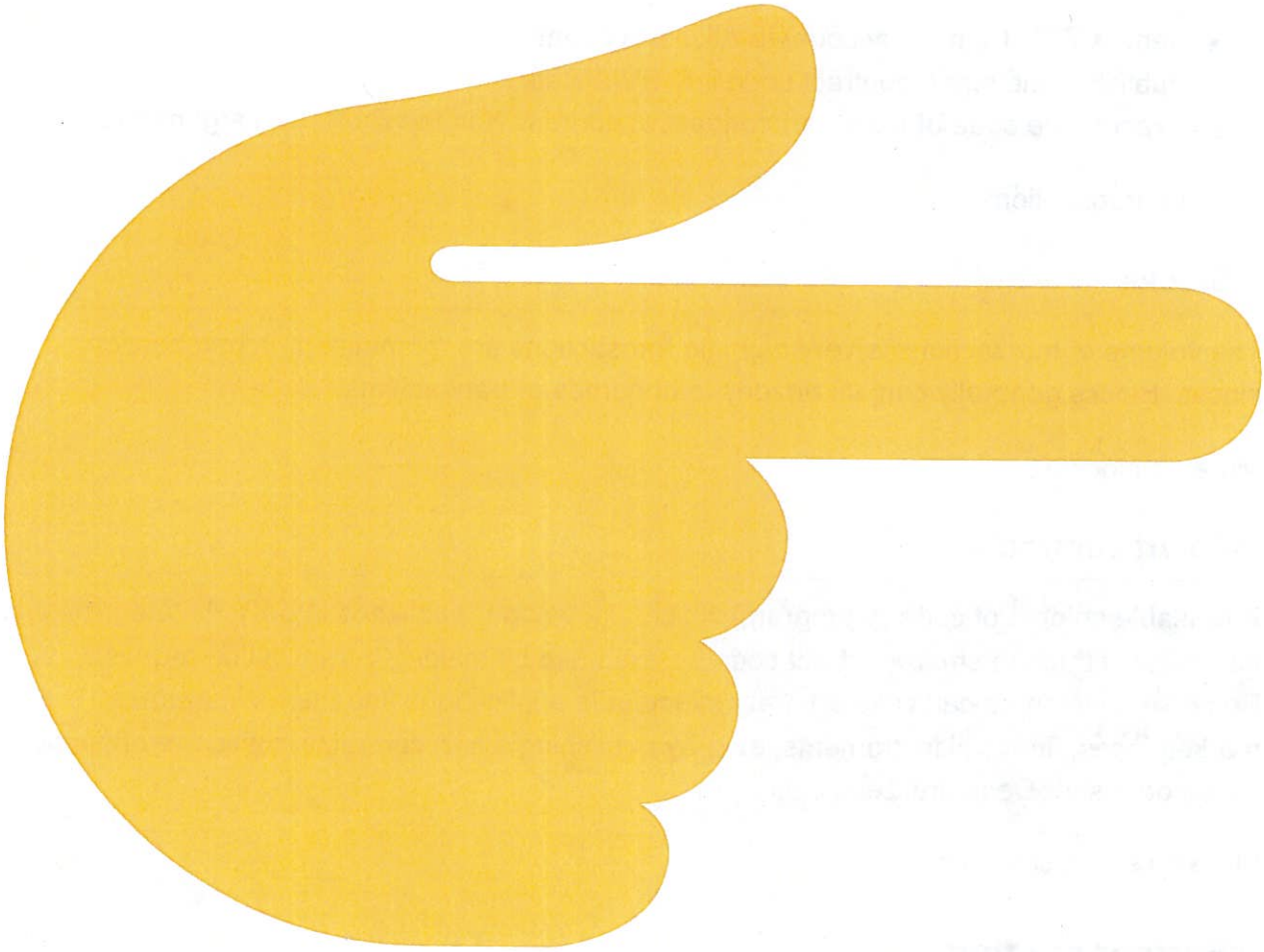


EXHIBIT 104

Practical Law™

Resource ID: W-021-8235

Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies

PRITESH SHAH AND DANIEL FORESTER, DAVIS POLK & WARDWELL LLP, AND MATTHIAS BERBERICH AND CAROLIN RASPÉ, HENGELER MUELLER, WITH PRACTICAL LAW DATA PRIVACY ADVISOR

A Practice Note discussing blockchain technology, recent trends in data privacy law, and the tensions between them. It explains blockchain technology's characteristics and describes issues and potential strategies for complying with the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) and the California Consumer Privacy Act of 2018 (CCPA), including anonymity and pseudonymity, data controller and data processor identification, territorial and cross-border data transfer issues, legitimate bases for processing personal data, and individuals' rights.

Blockchain is one of the most hyped developments to arrive on the technology scene in recent years. However, blockchain technology and data privacy laws and regulations have largely developed independently. Heightened global data protection regimes with dramatically increased potential fines drive businesses to further reevaluate their privacy practices. Significant ambiguity and complexity currently exist for organizations in applying data privacy requirements to blockchain technology and associated services.

This Note:

- Explains blockchain technology, including core elements and design choices.
- Considers key tensions and issues between using blockchain technology and data privacy laws and regulations.
- Offers potential steps for mitigating compliance risks.

BLOCKCHAIN TECHNOLOGY CHARACTERISTICS

Blockchain gained notoriety and quickly became part of popular parlance during 2017's unprecedented cryptocurrency boom.

The technology builds on longstanding concepts and techniques in distributed transaction processing and encryption. Software developers initially brought these ideas together in a remarkably innovative manner to support Bitcoin's 2009 launch, giving rise to the first "blockchain" network. Cryptocurrencies, many of which use the concepts Bitcoin introduced, continue to proliferate.

Astute observers quickly recognized the underlying technology's potential beyond its original use to record trustless, peer-to-peer transfers of value. Blockchain applications have grown, with current use cases in:

- Smart contract development.
- Supply chain management, asset registers, and recordkeeping tools.
- Other innovations in varied industries, including:
  - fintech;
  - real estate;
  - health care; and
  - retail.

Blockchain implementations share several core elements, regardless of use case or application, including:

- Distributed ledger technology. This software infrastructure provides a synchronized and shared data structure that multiple participants can access and modify over a peer-to-peer network. The ledger chronologically links each new published data block to previous blocks of transactions using a cryptographic hashing process to form a chain. Participants or nodes generally store a complete copy of the ledger with previous transactions.
- **Consensus mechanisms.** These algorithms typically require a defined majority of participants to verify the legitimacy of and agree on each new ledger transaction request, taking the place of a traditional centralized administrator. Some consensus models include:
  - proof-of-work, which, mostly in public blockchains, induces participants to compete for the right to verify and settle blocks of transactions by solving computationally intensive puzzles;
  - proof-of-stake, which sets block publishing rights according to participants' known investment in the blockchain; and

  - proof-of-authority, which verifies a participant's identity and authorization level before granting block publishing rights, typically in private blockchains of known participants.
- **Selection of public versus private participation.** Public or permissionless blockchains, like those supporting most cryptocurrencies, allow anyone in any location to participate, subject to the implementation's consensus mechanisms. Private or permissioned blockchains restrict who may access and participate in the network and particular transactions either automatically or through identified gatekeepers. Many business or enterprise applications require access controls or other limitations, such as restricting data content or storage locations, that private blockchains can offer. These applications, often with more centralized networks and smaller participant groups, benefit from blockchain characteristics but also share many features and risks with traditional centrally administered databases.
- **Transaction immutability.** Widely touted as a blockchain benefit, transaction immutability follows from the way the distributed ledger technology cryptographically links each new block to the previous entry. Participants must however consider immutability strength through the lens of the particular blockchain's characteristics, including security levels and other potential risks. For example, a "51% attack" occurs when bad actors compromise a majority of participants, overwhelm the consensus mechanism, and alter the blockchain contents for their benefit. The guarantee of immutability is stronger in large robust networks where the resources required to gain majority control make these attacks cost-prohibitive.

For more on blockchain technology characteristics, including other cybersecurity risks and issues, see Practice Note, Cybersecurity Tech Basics: Blockchain Technology Cyber Risks and Issues: Overview (w-017-1916).

RECENT TRENDS IN DATA PRIVACY LAW

Paralleling blockchain technology's growth over the past decade, data privacy has seen a sharp uptick in global attention as a general policy and regulatory concern. Changes in the EU and US especially have the potential to affect blockchain technology users, although these jurisdictions have historically approached data privacy in different ways. Specifically:

- The EU takes an omnibus approach with its General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), which entered into force on May 25, 2018. Its proposed EU E-Privacy Regulation further addresses electronic communications (see The EU's GDPR and Draft E-Privacy Regulation).
- The US conversely approaches data privacy in a patchwork, sector-specific fashion at the federal level. Some states have taken the lead by adopting broader legislation, for example, with the California Consumer Privacy Act of 2018 (CCPA) (see The CCPA and US Trends).

For a summary comparison of the GDPR and CCPA, see Practice Note, CCPA and GDPR Comparison Chart (w-016-7418).

These and other current regimes perpetuate a traditional data protection framework that challenges decentralized technologies like blockchain because they envision:

- Data controllers or businesses that determine the purposes for and means of processing, for instance, by collecting, using, and managing personal data at their discretion.
- Data processors or service providers that work on data controllers' behalf.

This longstanding notion of centralized entities that control both the data they collect and their service provider relationships contrasts with blockchain technology's distributed peer-to-peer network architecture.

THE EU'S GDPR AND DRAFT EU E-PRIVACY REGULATION

The GDPR sets out a high, harmonized personal data protection standard for the EU and the European Economic Area (EEA), although it allows member states to make some derogations.

The GDPR:

- Defines personal data broadly to include any information relating to an identified or identifiable individual (Article 4(1), GDPR).
- Takes an expansive extraterritorial view, protecting EU residents from less stringent data protection standards in other countries by applying to:
  - processing personal data of individuals in the EU when offering goods or services to those individuals in the EU; and
  - online behavioral monitoring of individuals in the EU.

Controllers and their optional processors must take various steps to document their programs and comply with the GDPR's principles and many obligations. Blockchain technology users may find several compliance requirements challenging, including:

- Ensuring the legality of personal data processing, for example, by:
  - obtaining individual data subjects' consent; or
  - meeting requirements for other legal bases like fulfillment of a contract or balancing of legitimate interests.

  (Article 6, GDPR.)
- Informing data subjects about and fulfilling various individuals' rights, such as:
  - notice;
  - data access, rectification, and portability;
  - opportunities to object to processing, including automated decision making; and
  - data removal, also known as "the right to be forgotten," under specified circumstances.

  (Articles 12 through 23, GDPR.)
- Maintaining risk-based data security standards (Article 32, GDPR).

The GDPR sets out high potential fines for noncompliance of up to the greater of EUR20 million or 4% of annual worldwide turnover (Article 83, GDPR). For more on the GDPR and its applicability, see Practice Notes, Overview of EU General Data Protection Regulation (w-007-9580) and Determining the Applicability of the GDPR (w-003-8899).

The current E-Privacy Directive (Directive 2002/58/EC), as amended by the EU Citizens' Rights Directive (Directive 2009/136/EC), further governs data protection for electronic communications. EU policymakers intend for the draft E-Privacy Regulation to

complement the GDPR. A final draft is expected in late 2019 at the earliest, making entry into force unlikely before 2020. Transitional periods may postpone its applicability.

The current draft E-Privacy Regulation indicates that it is likely to apply to:

- The processing of electronic communications data relating to the provision and use of electronic communications services.
- Information related to end users' terminal equipment.

The draft E-Privacy Regulation regulates data with a different scope than the GDPR, including only certain communications data like content and metadata regardless of whether it is personal data or not. Like the GDPR, data processing requires a legal basis by consent or law, such as processing that is technically necessary for providing communications services. Potential issues for blockchain technology users remain open. For example, as they are finalized, the draft E-Privacy Regulation provisions may further challenge online services using blockchain technology.

US TRENDS AND THE CCPA

The US has not yet implemented a comprehensive federal data protection framework, relying instead on sector-specific privacy and data security laws and regulations, such as:

- The Gramm-Leach-Bliley Act (GLBA) for financial institutions.
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) for health care providers, health plans, and their service providers.

For more on current US privacy and data security laws, see Practice Note, US Privacy and Data Security Law: Overview (6-501-4555).

Many observers expect Congress to eventually enact a more comprehensive privacy and data security law that may at least partially preempt state laws. In the meantime, states have taken the lead. For example, California enacted the most comprehensive and stringent state-level data protection law in the US to date with the CCPA. The new protections for California residents begin January 1, 2020. Similar legislation is under consideration in several other states (see Practice Note, 2019-2020 Federal and State Privacy-Related Legislation Tracker (w-020-3899)).

The CCPA:

- Defines personal information broadly to include any information that directly or indirectly identifies, describes, or can reasonably link to a particular California resident consumer or household (Cal Civ. Code § 1798.140(o)).
- With some exceptions, applies to businesses that collect and control consumers' personal information and meet at least one of the following thresholds:
  - annual gross revenue that exceeds $25 million (adjusted for inflation);
  - annually buys, receives, shares, or sells alone or in combination the personal information of more than 50,000 consumers, households, or devices for commercial purposes; or
  - derives 50% or more of annual revenues from selling consumers' personal information.

(Cal. Civ. Code § 1798.140(c)(1).)

Like the GDPR, the CCPA provides consumer protections and compliance obligations that may be challenging for blockchain technology users, including:

- Informing consumers about and fulfilling various individuals' rights, such as:
  - notice, access, and disclosure, including details regarding third-party disclosures or sales (Cal. Civ. Code §§ 1798.100, 1798.110, 1798.115, and 1798.130);
  - an opportunity to opt-out of sales of personal information without discrimination, or opt-in for minors (Cal. Civ. Code § 1798.120); and
  - the right to be forgotten, subject to certain limits (Cal. Civ. Code § 1798.105).
- Maintaining risk-based data security standards, enforced by a CCPA-granted private right of action regarding data breaches that result from a business's failure to maintain adequate data security standards (Cal. Civ. Code §§ 1798.81.5 and 1798.150).

The CCPA grants rulemaking and enforcement authority to the California Attorney General (CAG) with administrative penalties of up to $2,500 per violation and $7,500 per intentional violation that likely extend to each affected individual (Cal. Civ. Code § 1798.155(b)). It is not yet clear how the CAG intends to implement these fines.

For details on the CCPA and current amendment status, see Practice Notes, Understanding the California Consumer Privacy Act (CCPA) (w-017-4166) and CCPA Proposed Amendments and Other California Privacy-Related Legislation Tracker (w-020-3287).

TENSIONS BETWEEN BLOCKCHAIN TECHNOLOGY AND COMMON DATA PRIVACY REQUIREMENTS

Legislators do not appear to have focused on blockchain technology and its unique features when drafting recent data privacy laws and frameworks. Some blockchain technology features can help mitigate or cater to privacy concerns, such as using encryption and verifying data integrity. However, blockchain technology's distributed peer-to-peer network architecture often places it at odds with the GDPR's and CCPA's traditional notion of centralized controller-based data processing. This disconnect can make it difficult to reconcile current data protection laws with blockchain's other core elements, such as the lack of centralized control, immutability, and perpetual data storage. Regulatory guidance on reconciling this and other potential conflicts is currently limited.

Handling data privacy issues and properly applying laws, such as the GDPR and CCPA, increasingly contribute to a business venture's success or failure, including those that use blockchain technology. Circumstances may require or organizations may benefit from conducting a privacy impact assessment (PIA) or data protection impact assessment (DPIA) before implementation or release.

Some important tensions between blockchain technology and data privacy requirements to consider include:

- Different perspectives on anonymity and pseudonymity and how they affect the applicability of various data protection and privacy laws (see Anonymity, Pseudonymity, and Privacy Law Applicability).
- How to identify data controllers and data processors in various blockchain technology implementations (see Data Controller and Data Processor Identification).

- Territorial implications for distributed blockchain networks (see Territorial Considerations).
- When cross-border data transfers occur and potential restrictions on them (see Cross-Border Data Transfers).
- Applying criteria for legitimate reasons for processing personal data to blockchain use cases (see Legitimate Reasons for Processing Personal Data).
- Reconciling transaction immutability and data preservation in blockchain applications with individuals' rights (see Immutability and Individuals' Rights).

For more on PIAs, DPIAs, the commonality between them and a template, see Practice Note, Conducting Privacy Impact Assessments (w-012-5912) and Standard Document, Privacy Impact Assessment (w-012-5914).

ANONYMITY, PSEUDONYMITY, AND PRIVACY LAW APPLICABILITY

The applicability of most data privacy laws, including the GDPR and the CCPA, depends first on whether the activities in question involve the processing of personal data. Blockchain implementations that expressly record personal data on the blockchain are clearly subject to laws regarding personal data. However, whether the data some blockchains record, process, or use to manage transactions qualifies as personal data varies. For example:

- Blockchains may expressly include personal data as "payload" if they aim to create a record of ownership or other assigned rights that require sufficient identifying information.
- Blockchains, including many public blockchains that support popular cryptocurrencies, tout anonymity or at least some level of privacy by using public-private key pair encryption. These asymmetric encryption systems:
  - leverage the mathematical relationship between the public and private keys in a particular pair;
  - record public keys on the blockchain implementation;
  - do not typically record public key owner data or other similar personal information; and
  - leave users to retain and protect their own private keys.

Some blockchain enthusiasts claim that using public-private key encryption preserves anonymity and privacy. This is a relatively simplistic view of personal information that may not hold up under GDPR or CCPA definitions because:

- Methods exist for linking individuals to public keys by analyzing blockchain transactions and other publicly available data. Some businesses offer services to identify individuals using their public keys, blockchain transactions, and other available data.
- The GDPR defines personal data broadly (see The EU's GDPR and Draft E-Privacy Regulation). The threshold for identification is low, recognizing any means "reasonably likely to be used," considering all objective factors, such as costs and time, and available and anticipated technology (Recital 26, GDPR). The GDPR also includes online identifiers, which the European Court of Justice (ECJ) previously addressed in its *Breyer v. Germany* decision (Case 582/14), holding that dynamic IP addresses are personal data (see Practice Note, Overview of EU General Data Protection Regulation: Online identifiers (w-007-9580)).
- The CCPA takes a similarly broad view of personal information that includes:
  - "online identifiers," without specific definition; and
  - unique identifiers that encompass "persistent or probabilistic identifiers that can be used to identify a particular consumer or device" (Cal. Civ. Code § 1798.140(x)).

See Practice Note, Understanding the California Consumer Privacy Act (CCPA) : Personal Information Under the CCPA (w-017-4166).

Better practice treats public keys as tokenizations of personal information from a privacy perspective instead of anonymized data, because:

- They correspond to an individual.
- Reidentification becomes possible in some circumstances.

Blockchain technologists also sometimes claim that their implementations are anonymous because they record transaction data that:

- Only references a public blockchain address and not the underlying owner's name or other directly identifiable personal information.
- Often do not display unencrypted public blockchain addresses.

This usage again contrasts with data privacy laws that only consider personal information anonymized or deidentified if it cannot be reasonably linked to an identifiable individual. Applying pseudonymization techniques lowers risk but does not remove regulatory obligations. For more on these techniques under the GDPR, see Practice Note, Anonymization and Pseudonymization Under the GDPR (w-007-4624).

Reidentification risks and related concerns have led some blockchains, including privacy-focused cryptocurrencies, to try to reduce the risk of identifying individual participants by:

- Implementing various mitigation strategies to protect transaction and other data.
- Introducing alternative cryptographic approaches.

Organizations should consider the applicability of the GDPR, the CCPA, and other data privacy laws to proposed blockchain use cases by:

- Carefully assessing specific blockchain implementation details.
- Reviewing potential reidentification methods and risks.
- Monitoring emerging guidance.

DATA CONTROLLER AND DATA PROCESSOR IDENTIFICATION

Blockchain implementations that process personal information are at odds with the clear distinction that data privacy laws and frameworks, like the GDPR and CCPA, make between:

- Controllers and their processors.
- Individual data subjects.

The distributed peer-to-peer network architecture means that it is often unclear which party determines the purposes and means of processing.

Private blockchains present a simpler case. Here a central operator or consortium likely qualifies as a controller or joint controllers if they:

- Have control over the blockchain system, like a traditional system architecture.
- Determine the purposes and means for any personal data processing.

Other actors that help operate the blockchain specifically for the central operator, such as nodes or miners, can take the processor role. The private blockchain operator or consortium must implement appropriate data processing agreements or other contracts to hold these service providers accountable and meet regulatory obligations. Alternatively, private blockchains where the central operator performs all technical support activities may not have data processors or service providers by default.

Public blockchains typically lack a central operator, making it difficult to assign traditional controller and processor accountability. For example:

- Each public blockchain node independently processes the same transaction data set, at least during the block verification process. This might lead to classification of each blockchain node as a joint controller under the GDPR, but authorities and commentators alike are reluctant to draw this conclusion for all nodes (Articles 4(7) and 26, GDPR; see CNIL Guidance).
- Conversely, if no entity has clear control over the data, then participants may try to argue that there is no controller and hence there can be no processors. However, this argument may not be compatible with the GDPR, because the GDPR emphasizes a "clear allocation of responsibilities" for personal data processing (Recital 79, GDPR).

Data protection authorities and other regulators have been slow to address blockchain technology, except for the French data protection authority (*Commission Nationale de l'informatique et des Libertés* (CNIL)) (see CNIL Guidance).

Businesses that use blockchain technology when collecting or managing personal data should carefully analyze their accountability under applicable regulations, including the roles any service providers they engage play.

CNIL Guidance

The CNIL has issued initial cautious guidance on applying the GDPR to some blockchain technology use cases. The CNIL guidance focuses on various blockchain actors, distinguishing among:

- Participants that have full writing rights to enter transactions on the blockchain and to send the data for validation to miners.
- Accessors that may retain full copies of a blockchain but have read-only rights.
- Miners that validate transactions and create new blocks according to the implementation's governance model.

Participants under these distinctions are controllers regarding personal data they enter on a blockchain, because in doing so, they determine the purposes and means for processing. Mere accessors and miners normally do not make these determinations and so are not controllers. The CNIL guidance also notes that individuals entering personal data on a blockchain for strictly personal purposes are not controllers under the GDPR's household exception (Article 2, GDPR).

However, when third parties act on a participant's behalf, they may become processors and then should enter into data processing agreements.

Regarding miners, the CNIL guidance notes that:

- Miners that are only validating transactions and are not involved in the object of those transactions, for instance, miners just building new blocks according to the technical protocol, are not controllers in the CNIL's view.
- In some cases, miners may be data processors in the CNIL's view, if they follow a data controller's instructions, for example, in a private blockchain of insurance companies that mine transactions on behalf of customers.

Although this may suggest that in certain circumstances miners may be neither a data controller nor a data processor, the CNIL guidance is not clear.

TERRITORIAL CONSIDERATIONS

Data privacy laws often apply according to either or both:

- The individual's location.
- The personal data processing location.

For example:

- The CCPA is indifferent to a business's processing location if it involves the personal information of California residents.
- The GDPR applies:
  - to personal data processing activities by either controllers or processors established in the EU or the broader EEA; and
  - regardless of location, if the personal data processing involves offering individuals goods or services in the EU or online behavioral monitoring of individuals in the EU.

(See The EU's GDPR and Draft E-Privacy Regulation.)

Evaluating jurisdictionality and applying regulations to decentralized blockchain implementations is not a straightforward exercise compared to traditional centralized systems.

More cautious blockchain projects that handle personal data may try to limit participants by jurisdiction, although reliably confirming online locations can be difficult. Private blockchains more often set restrictions in their governance models and agreements to limit regulatory scope. Public blockchains that process personal data may assume applicability for various regulatory regimes as a best practice, but:

- Managing the diverse set of regulations can incur significant overhead costs.
- Using common public-private key pairing for encryption may bring them in many regimes' scope (see Anonymity, Pseudonymity, and Privacy Law Applicability).

CROSS-BORDER DATA TRANSFERS

The distributed nature of blockchain technology not only poses a challenge regarding the applicability of various jurisdictions' laws, but it also raises tensions with those that restrict cross-border data transfers. Most notably, the GDPR:

- Permits personal data transfers to countries outside the EEA only under specific circumstances.

- Requires specific safeguards in the recipient jurisdiction to ensure the same or an adequate level of protection.

Controllers must implement additional safeguards unless the European Commission issues an adequacy decision for the recipient location. Safeguards may take the form of standard contractual clauses, binding corporate rules, codes of conduct, or certification mechanisms. For more on cross-border data transfers under the GDPR, see Practice Note, Overview of EU General Data Protection Regulation: Cross-border data transfers (w-007-9580).

These safeguards:

- Normally require some centralized compliance program to implement them.
- Are especially difficult to consider implementing in public blockchains with their undefined participant groups.

Other jurisdictions are increasingly seeking to limit cross-border data transfers and may call for similar protective mechanisms.

LEGITIMATE REASONS FOR PROCESSING PERSONAL DATA

Some data protection and data privacy laws limit the permitted uses of or require legitimate reasons for processing personal data. For example:

- Federal sector-specific laws in the US, like the GLBA and HIPAA, and various state laws limit certain personal data use without individuals' consent. Various exceptions may apply, such as HIPAA's permitted uses for treatment, payment, and health care operations (45 C.F.R. § 164.506).
- The GDPR only allows controllers to process personal data based on one or more lawful purposes, including data subjects' consent or processing to the extent necessary for:
  - entering or performing a contract with the data subject;
  - complying with the controller's legal obligations;
  - protecting vital interests of the data subject or another natural person;
  - performing public interest or official tasks; or
  - pursuing the controller's or a third party's legitimate interests unless the data subject's interests or fundamental rights and freedoms override them;

  (Article 6, GDPR.) For more on the GDPR's legal processing grounds, see Practice Note, Overview of EU General Data Protection Regulation: Lawfulness of processing (w-007-9580).

It is unclear whether these options encompass perpetual distributed blockchain storage. Blockchain participants may request consent from their users or data subjects, as applicable. However:

- In some instances, it may be preferable for controllers under the GDPR to depend on a basis other than consent because it must be:
  - freely given;
  - specific;
  - informed; and
  - unambiguous.

  (Article 4(11), GDPR.)
- Even if consent mechanisms meet GDPR or other relevant standards:
  - individuals can withdraw consent at any time without reason; and
  - blockchains may store personal data in a way that is extremely difficult to remove making later processing unlawful.

Organizations must carefully consider scenarios like consent withdrawal when determining what data they store in blockchain applications and how they record it.

IMMUTABILITY AND INDIVIDUALS' RIGHTS

Data privacy laws increasingly grant individuals with rights, aiming to:

- Help individuals regain a measure of control over their personal data.
- Allow individuals to choose to protect their personal data from monetization or exploitation without their consent or other justification.

For more on data subject rights under the GDPR and CCPA, see Recent Trends in Data Privacy Law.

Rights of data correction and data erasure, also known as the right to be forgotten, present the most apparent conflict with blockchain technology's transaction immutability characteristics. Blockchains, in particular implementations that provide ownership, supply chain, and other recordkeeping tools, including smart contracts, can likely address data updates by recording additional transactions. However, these later transactions do not technically delete data previously stored on the blockchain. The same approach supports updating various process steps and status values.

Whether blockchain technology fundamentally conflicts with the right to be forgotten depends on how strictly authorities interpret "erasure." A strict technical erasure of blockchain data, in a current standard blockchain architecture, requires both:

- A backward deconstruction of the blockchain up to and including the targeted record.
- A reconstruction of the blockchain from the point of the deleted data forward.

This kind of operation:

- Conflicts with basic blockchain design principles.
- Consumes significant processing resources from participants.
- Requires consent from the necessary threshold of participants or according to other rules in the blockchain's governance model (see Blockchain Technology Characteristics).
- Would therefore be feasible only as an extreme exception in operation, comparable in its efforts to a "hard fork" in public blockchain communities, where a group decides to split the code of a particular blockchain and run a modified, parallel implementation.

These strict technical data deletion measures:

- Are very difficult to implement every time individuals seek to exercise their rights.
- May be more feasible in private blockchain governance models with a central operator.

POTENTIAL MITIGATING STEPS

Some have called for legislative updates or at least guidance from relevant authorities to reconcile data privacy laws with emerging decentralized technologies like blockchain. For now, organizations should follow several risk management strategies when considering blockchain technology by:

- Carefully evaluating whether using blockchain technology is a good fit for current business and processing objectives, as even early commenting regulators like the CNIL have emphasized (see CNIL Guidance).
- Preferring private or permissioned blockchains to enforce stricter usage rules (see Use Permissioned Blockchains to Support Governance Models).
- Using data structure and design techniques to limit the personal data they actually store on blockchains (see Avoid or Limit Personal Data Stored on Blockchains).
- Adopting alternative data encryption and destruction techniques to protect personal data (see Use Alternative Data Encryption and Destruction Approaches).

USE PERMISSIONED BLOCKCHAINS TO SUPPORT GOVERNANCE MODELS

Public permissionless blockchains reflect the technology's original notions and benefits of permitting any individual to access, view, and submit transactions with minimal data governance. Organizations must balance these benefits with their needs to follow consistent data privacy practices and comply with applicable laws and regulations.

One commonly proposed way to foster consistent participant practices and regulatory compliance encourages organizations to:

- View the differences between public permissionless and private permissioned blockchain implementations as a spectrum rather than a binary decision.
- Implement a blockchain architecture that lies closer to the private permissioned end of the spectrum.

These increasingly adopted implementations can employ various governance structures and processes to:

- Authorize a select number of vetted and approved participants.
- Ensure that the authorized participants follow strict consensus practices for data privacy.
- Take technical measures to further reduce and regulate the amount of personal data that participants process.

Using blockchain technology for business applications with lower numbers of authorized participants has pros and cons. For example, a lower number of participants:

- Theoretically makes it easier for one participant to overwhelm the blockchain's consensus mechanism depending on its characteristics (see Blockchain Technology Characteristics).
- Conversely may heighten security because:
  - participants can contractually bind each other regarding their usage; and
  - misbehavior is not anonymous and is easy to link to identifiable participants.

More centralized control over the blockchain implementation may also permit more traditional contractual approaches to:

- Allocating data processing responsibility and accountability.
- Managing cross-border data transfers.
- Responding to individuals' and authorities' requests.
- Deploying data processing agreements between those playing controller and processor roles.

AVOID OR LIMIT PERSONAL DATA STORED ON BLOCKCHAINS

One way to address laws and regulations that hinge on personal data is to avoid putting any personal data on a blockchain. However, the broad definitions for personal data across various regimes make it challenging to fully avoid falling in their scope, especially in blockchains that use public-private key encryption to manage transactions among individuals (see Anonymity, Pseudonymity, and Privacy Law Applicability).

Use cases particularly suited to avoiding data capable of directly or indirectly identifying an individual include:

- Financial settlement systems that do not involve natural persons.
- Supply chain management.
- Managing distributed internet of things (IoT) non-personal sensor data.
- Other applications that do not handle information on natural persons.

For use cases that involve personal data, organizations should consider using more privacy-friendly blockchain techniques, such as those that:

- Combine on-chain and off-chain storage to:
  - avoid storing personal data as a payload on the blockchain; and
  - allow blockchain transactions to serve as mere pointers or other access control mechanisms to more readily managed storage solutions.

Future technologies may further strengthen privacy for blockchains that handle personal data by making individual user identification harder. For example:

- Some have suggested adding noise to blockchain data, mixing up transactions, or using groups of encryption keys to avoid reidentification.
- Others, including the emerging MimbleWimble protocol and the privacy-friendly cryptocurrency Grin, leverage encryption techniques that allow participants to:
  - prove that they know something without revealing the nature and identity of the information; and
  - use one-time addresses that do not require archiving.

These privacy-friendly techniques may run into additional regulatory concerns, especially for cryptocurrencies or other financial transactions, including know your customer, anti-money laundering, and anti-terrorism laws and regulations.

USE ALTERNATIVE DATA ENCRYPTION AND DESTRUCTION APPROACHES

Alternative data encryption and destruction approaches may help address compliance concerns regarding personal data on blockchains and address individuals' rights by using:

- Hashing or other irreversible data transformations.
- Destruction of separately stored hashing or encryption keys.
- Revocation of access rights.
- Other similar technical mechanisms.

Whether these mechanisms can meet regulators' demands for erasure remains to be seen, although the CNIL's guidance considers some of them as moving closer to the effect of data erasure (see CNIL Guidance). These techniques are typically easier to implement in private, permissioned blockchain systems, encouraging organizations to combine risk mitigation techniques.

THE FUTURE OF BLOCKCHAIN PRIVACY MANAGEMENT

Many current blockchain technology applications appear at least ambiguous from a privacy compliance perspective. Processing personal data directly on a public blockchain may, in the absence of clear regulatory guidance, involve significant business risks.

Looking forward, some technologists suggest that blockchain technology, with its data transparency and integrity features, offers unique possibilities to improve privacy by:

- Verifying and managing consent.
- Providing individuals with clear notifications and records of personal data usage across distributed systems.
- Minimizing data sharing between data controllers and their processors.

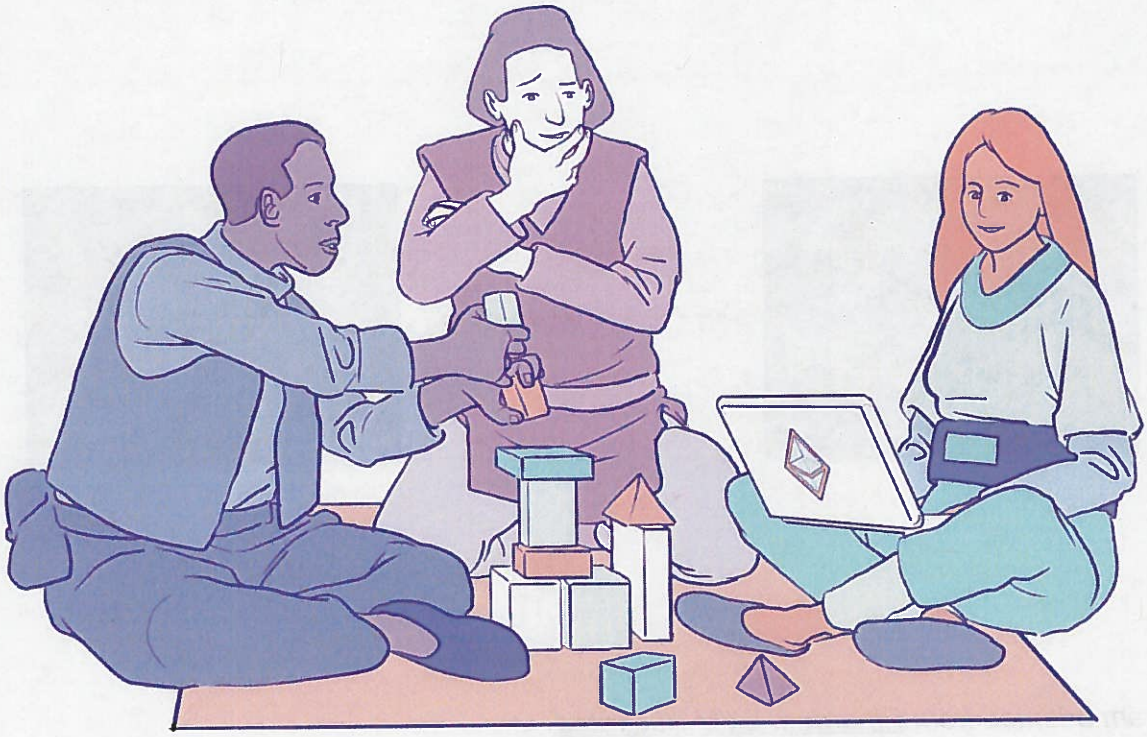
Taking this one step further, some researchers envision a future when self-governing blockchain-enabled identity and data management solutions provide the preferred way to maintain and demonstrate data privacy. For now, policymakers can support innovation by recognizing decentralized data storage models and better tailoring data privacy laws, regulations, and guidance for blockchain use cases.

10-19

EXHIBIT 107

Transactions

ethereum.org/en/developers/docs/transactions/



Last edit: , Invalid DateTime

Edit page

On this page

Transactions are cryptographically signed instructions from accounts. An account will initiate a transaction to update the state of the Ethereum network. The simplest transaction is transferring ETH from one account to another.

Prerequisites

To help you better understand this page, we recommend you first read Accounts and our introduction to Ethereum.

What's a transaction?

An Ethereum transaction refers to an action initiated by an externally-owned account, in other words an account managed by a human, not a contract. For example, if Bob sends Alice 1 ETH, Bob's account must be debited and Alice's must be credited. This state-changing action takes place within a transaction.

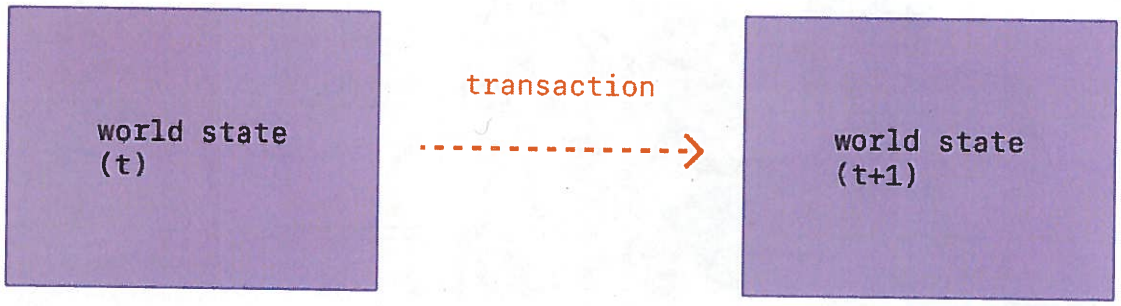


Diagram adapted from Ethereum EVM illustrated

Transactions, which change the state of the EVM, need to be broadcast to the whole network. Any node can broadcast a request for a transaction to be executed on the EVM; after this happens, a validator will execute the transaction and propagate the resulting state change to the rest of the network.

Transactions require a fee and must be included in a validated block. To make this overview simpler we'll cover gas fees and validation elsewhere.

A submitted transaction includes the following information:

- `recipient` – the receiving address (if an externally-owned account, the transaction will transfer value. If a contract account, the transaction will execute the contract code)
- `signature` – the identifier of the sender. This is generated when the sender's private key signs the transaction and confirms the sender has authorized this transaction
- `nonce` - a sequencially incrementing counter which indicate the transaction number from the account
- `value` – amount of ETH to transfer from sender to recipient (in WEI, a denomination of ETH)
- `data` – optional field to include arbitrary data

- `gasLimit` – the maximum amount of gas units that can be consumed by the transaction. Units of gas represent computational steps
- `maxPriorityFeePerGas` - the maximum amount of gas to be included as a tip to the validator
- `maxFeePerGas` - the maximum amount of gas willing to be paid for the transaction (inclusive of `baseFeePerGas` and `maxPriorityFeePerGas`)

Gas is a reference to the computation required to process the transaction by a validator. Users have to pay a fee for this computation. The `gasLimit` , and `maxPriorityFeePerGas` determine the maximum transaction fee paid to the validator. More on Gas.

The transaction object will look a little like this:

```
1{
2  from: "0xEA674fdDe714fd979de3EdF0F56AA9716B898ec8",
3  to: "0xac03bb73b6a9e108530aff4df5077c2b3d481e5a",
4  gasLimit: "21000",
5  maxFeePerGas: "300",
6  maxPriorityFeePerGas: "10",
7  nonce: "0",
8  value: "10000000000"
9}
10
```

Show all

Copy

But a transaction object needs to be signed using the sender's private key. This proves that the transaction could only have come from the sender and was not sent fraudulently.

An Ethereum client like Geth will handle this signing process.

Example JSON-RPC call:

```
{
  "id": 2,
  "jsonrpc": "2.0",
  "method": "account_signTransaction",
  "params": [
    {
      "from": "0x1923f626bb8dc025849e00f99c25fe2b2f7fb0db",
      "gas": "0x55555",
      "maxFeePerGas": "0x1234",
      "maxPriorityFeePerGas": "0x1234",
      "input": "0xabcd",
      "nonce": "0x0",
      "to": "0x07a565b7ed7d7a678680a4c162885bedbb695fe0",
      "value": "0x1234"
    }
  ]
}
```

Show all

Copy

Example response:

```
1{
2  "jsonrpc": "2.0",
3  "id": 2,
4  "result": {
5    "raw":
"0xf883800182033394 07a565b7ed7d7a678680a4c162885bedbb695fe080a44401a6e4000000000000000
6    "tx": {
7      "nonce": "0x0",
8      "maxFeePerGas": "0x1234",
9      "maxPriorityFeePerGas": "0x1234",
10      "gas": "0x55555",
11      "to": "0x07a565b7ed7d7a678680a4c162885bedbb695fe0",
12      "value": "0x1234",
13      "input": "0xabcd",
14      "v": "0x26",
15      "r": "0x223a7c9bcf5531c99be5ea7082183816eb20cfe0bbc322e97cc5c7f71ab8b20e",
16      "s": "0x2aadee6b34b45bb15bc42d9c09de4a6754e7000908da72d48cc7704971491663",
17      "hash": "0xeba2df809e7a612a0a0d444ccfa5c839624bdc00dd29e3340d46df3870f8a30e"
```

```
18    }
19  }
20}
21
```

Show all

Copy

- the `raw` is the signed transaction in Recursive Length Prefix (RLP) encoded form
- the `tx` is the signed transaction in JSON form

With the signature hash, the transaction can be cryptographically proven that it came from the sender and submitted to the network.

The data field

The vast majority of transactions access a contract from an externally-owned account. Most contracts are written in Solidity and interpret their data field in accordance with the application binary interface (ABI).

The first four bytes specify which function to call, using the hash of the function's name and arguments. You can sometimes identify the function from the selector using this database.

The rest of the calldata is the arguments, encoded as specified in the ABI specs.

For example, lets look at this transaction. Use **Click to see More** to see the calldata.

The function selector is `0xa9059cbb`. There are several known functions with this signature. In this case the contract source code has been uploaded to Etherscan, so we know the function is `transfer(address,uint256)`.

The rest of the data is:

```
1000000000000000000000004f6742badb049791cd9a37ea913f2bac38d01279

2000000000000000000000000000000000000000000000003b0559f4

3
```

According to the ABI specifications, integer values (such as addresses, which are 20-byte integers) appear in the ABI as 32-byte words, padded with zeros in the front. So we know that the `to` address is `4f6742badb049791cd9a37ea913f2bac38d01279`. The `value` is 0x3b0559f4 = 990206452.

Types of transactions

On Ethereum there are a few different types of transactions:

- Regular transactions: a transaction from one account to another.
- Contract deployment transactions: a transaction without a 'to' address, where the data field is used for the contract code.
- Execution of a contract: a transaction that interacts with a deployed smart contract. In this case, 'to' address is the smart contract address.

On gas

As mentioned, transactions cost gas to execute. Simple transfer transactions require 21000 units of Gas.

So for Bob to send Alice 1 ETH at a `baseFeePerGas` of 190 gwei and `maxPriorityFeePerGas` of 10 gwei, Bob will need to pay the following fee:

```
1(190 + 10) * 21000 = 4,200,000 gwei

2--or--

30.0042 ETH

4
```

Bob's account will be debited **-1.0042 ETH** (1 ETH for Alice + 0.0042 ETH in gas fees)

Alice's account will be credited **+1.0 ETH**

The base fee will be burned **-0.00399 ETH**

Validator keeps the tip **+0.000210 ETH**

Gas is required for any smart contract interaction too.

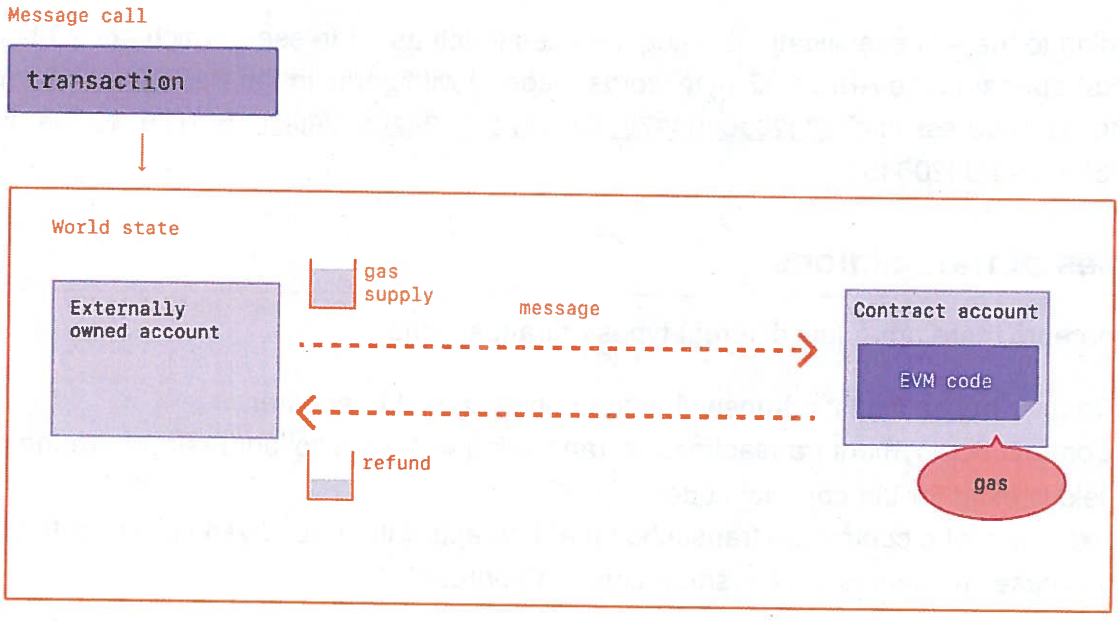


Diagram adapted from Ethereum EVM illustrated

Any gas not used in a transaction is refunded to the user account.

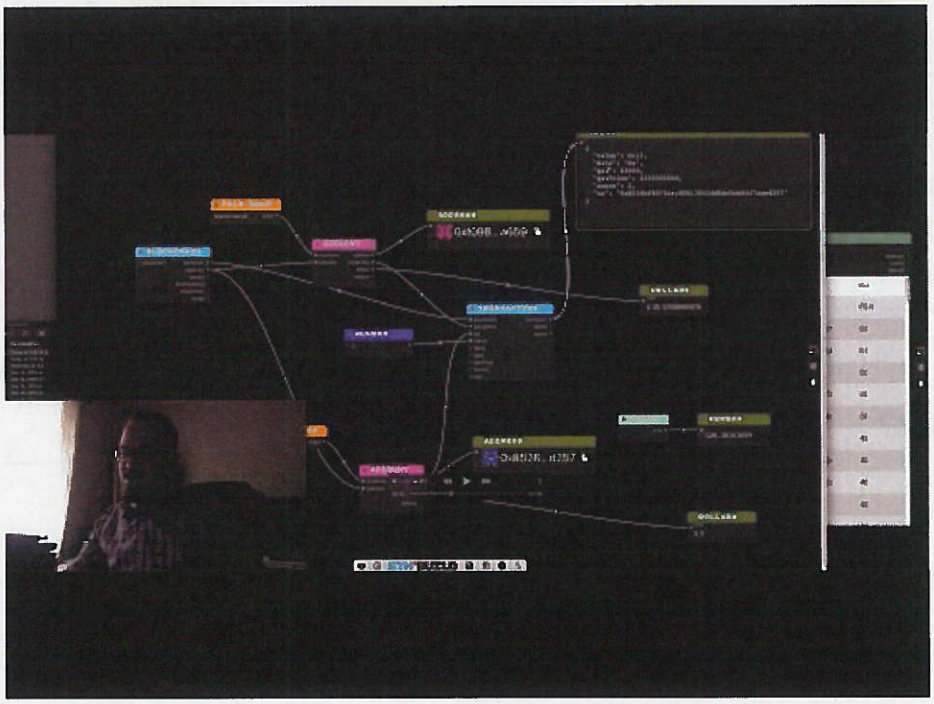
Transaction lifecycle

Once the transaction has been submitted the following happens:

1. Once you send a transaction, cryptography generates a transaction hash:
   `0x97d99bc7729211111a21b12c933c949d4f31684f1d6954ff477d0477538ff017`
2. The transaction is then broadcast to the network and included in a pool with lots of other transactions.
3. A validator must pick your transaction and include it in a block in order to verify the transaction and consider it "successful".
4. As time passes the block containing your transaction will be upgraded to "justified" then "finalized". These upgrades make it much more certain that your transaction was successful and will never be altered. Once a block is "finalized" it could only ever be changed by an attack that would cost many billions of dollars.

A visual demo

Watch Austin walk you through transactions, gas, and mining.



Watch Video At: https://youtu.be/er-0ihqFQB0

Typed Transaction Envelope

Ethereum originally had one format for transactions. Each transaction contained a nonce, gas price, gas limit, to address, value, data, v, r, and s. These fields are RLP-encoded, to look something like this:

```
RLP([nonce, gasPrice, gasLimit, to, value, data, v, r, s])
```

Ethereum has evolved to support multiple types of transactions to allow for new features such as access lists and EIP-1559 to be implemented without affecting legacy transaction formats.

EIP-2718: Typed Transaction Envelope defines a transaction type that is an envelope for future transaction types.

EIP-2718 is a new generalised envelope for typed transactions. In the new standard, transactions are interpreted as:

```
TransactionType || TransactionPayload
```

Where the fields are defined as:

- `TransactionType` - a number between 0 and 0x7f, for a total of 128 possible transaction types.
- `TransactionPayload` - an arbitrary byte array defined by the transaction type.

Further reading

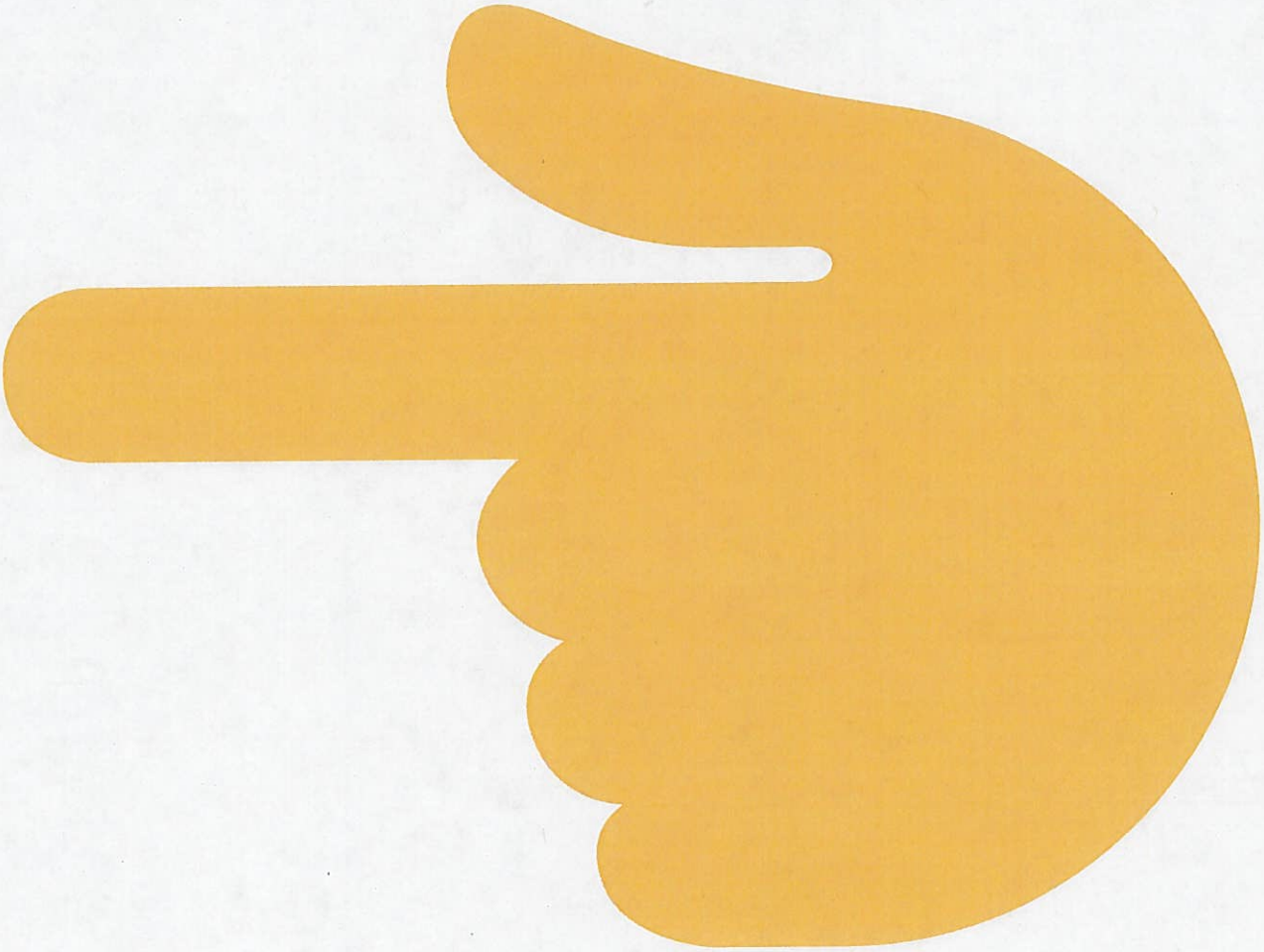
EIP-2718: Typed Transaction Envelope

Know of a community resource that helped you? Edit this page and add it!

Related topics

Back to top ↑

Was this article helpful?



Previous

Accounts
Next

Blocks

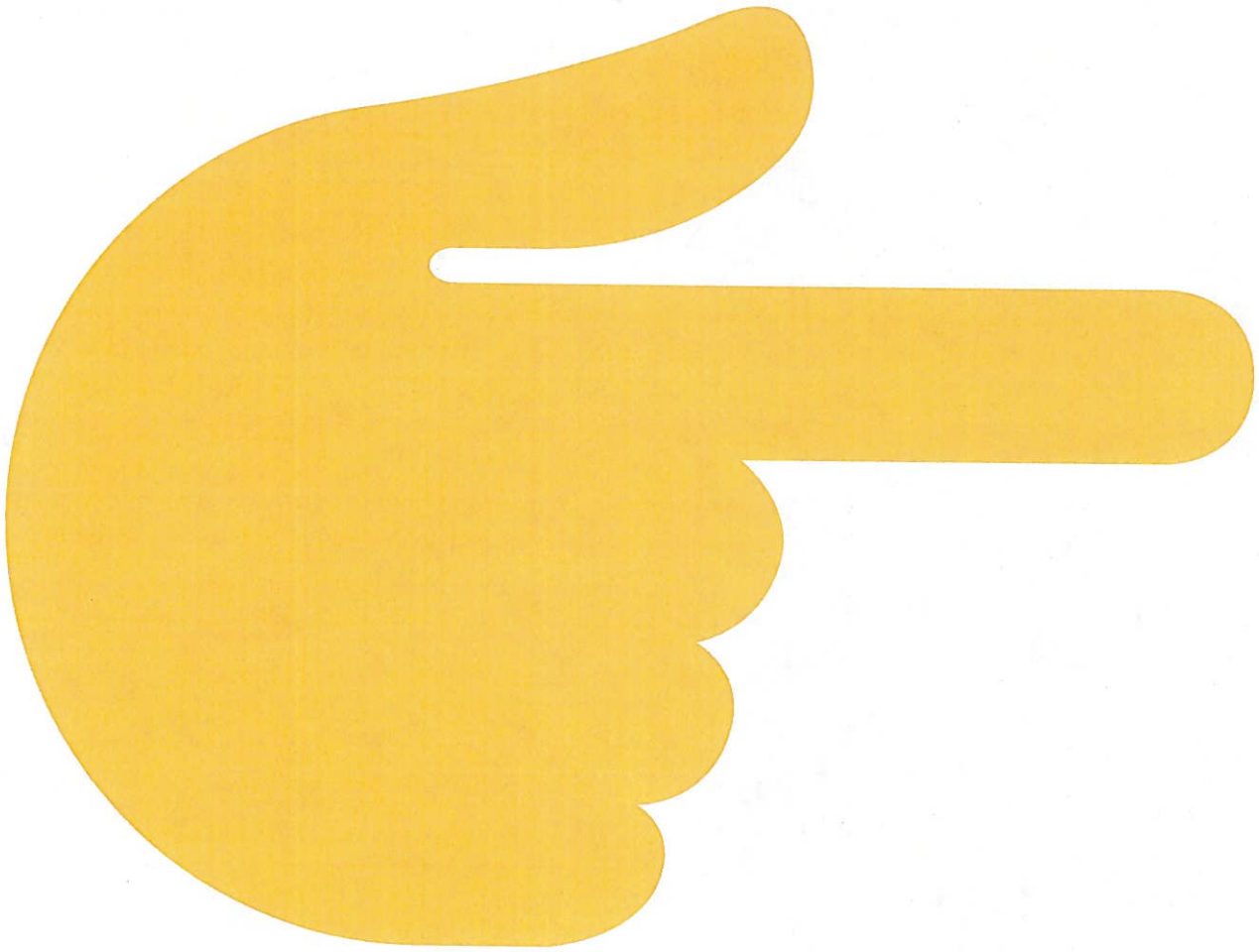
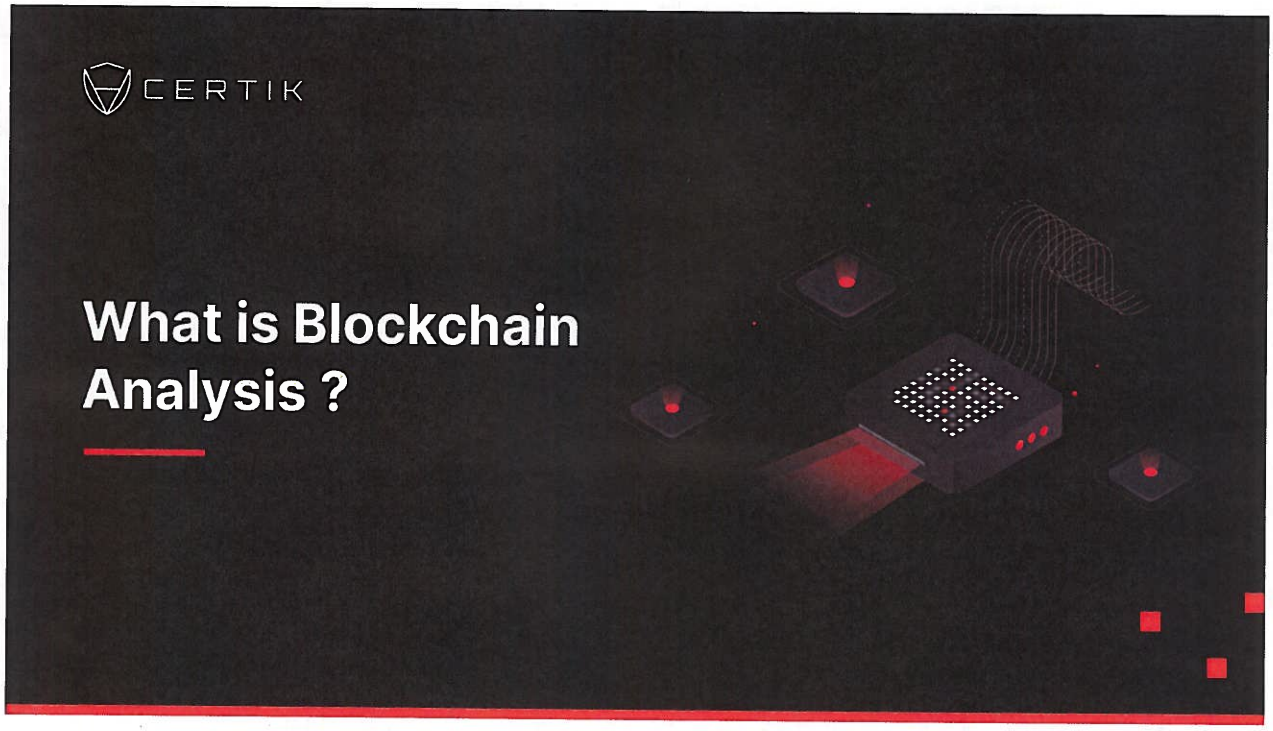


EXHIBIT 108

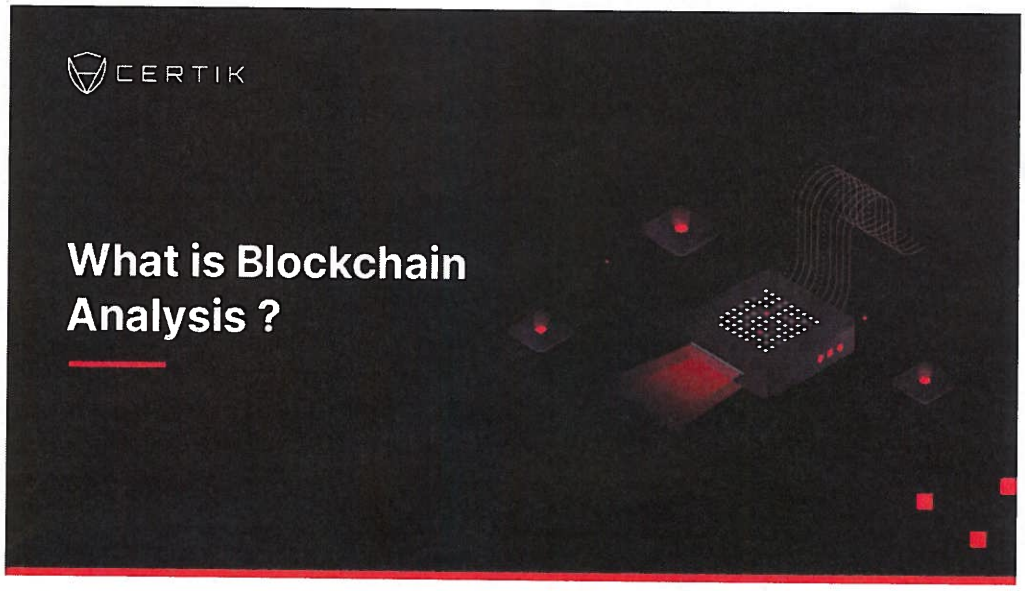
[redacted]

What is Blockchain Analysis? - Blog

certik.com/resources/blog/what-is-blockchain-analysis



← Back to all stories

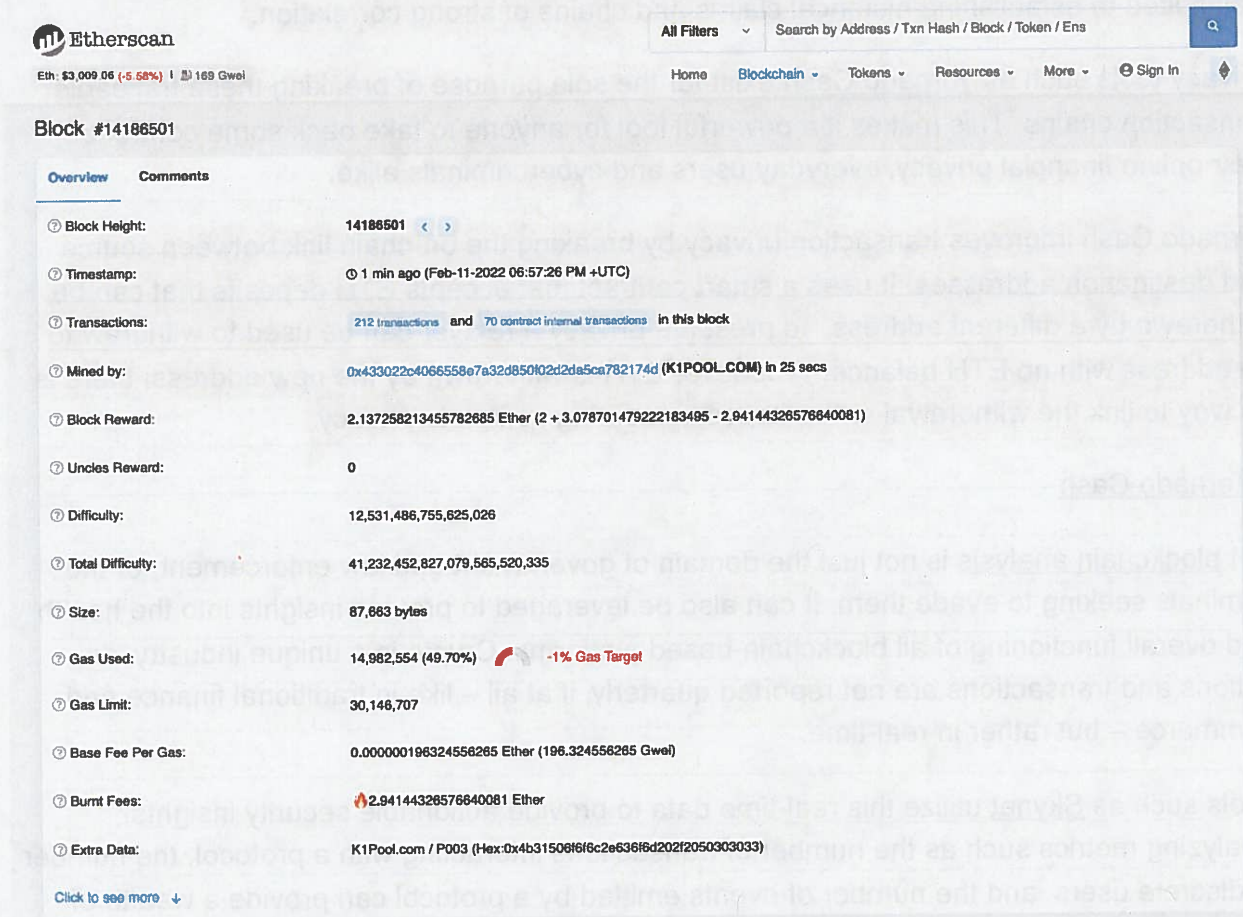


Blockchain analysis is the process of inspecting, cataloging, and interpreting the data that blockchains produce in order to gain actionable insights.

A public blockchain, such as Bitcoin or Ethereum, is essentially a database of accounts and their respective balances. Each new block in the chain updates the previous state of the database. With the Ethereum blockchain currently growing at a rate of more than 100GB per year, this represents an enormous amount of information added to the permanent history of the chain. And keep in mind that all this data is in text format, and 100GB of text is very different to 100GB of images or video.

This information is free for anyone and everyone to browse, but it exists in a raw, unprocessed state.

Tools such as blockchain explorers perform the fundamental tasks of organizing this data.



An Ethereum block's data on Etherscan

Block height, total difficulty, hashes, parent hashes, state roots, nonces... it's hard for anyone who doesn't make a career of blockchain analysis to differentiate between the useful and irrelevant information that blockchains create.

What Can You Do With Blockchain Analysis?

Before we get into how you can perform blockchain analysis, let's discuss why you might want to.

One of the primary purposes of blockchain analysis is to trace the flow of funds between addresses. This may be to follow the proceeds of an exploit, or to establish a transaction chain linking two or more wallets. Law enforcement agencies, such as the U.S. Department of Justice's newly launched National Cryptocurrency Enforcement Team (NCET), make extensive use of blockchain analysis when conducting anti-money laundering and cybersecurity operations. While no laws exist at the federal level regarding the admissibility of blockchain data in court cases, states including Arizona have passed laws confirming the legal validity of blockchain records. The immutability of blockchains makes the technology well-suited to establishing historical claims and chains of strong correlation.

Privacy tools such as Tornado Cash exist for the sole purpose of breaking these traceable transaction chains. This makes it a powerful tool for anyone to take back some control of their online financial privacy, everyday users and cybercriminals alike.

Tornado Cash improves transaction privacy by breaking the on-chain link between source and destination addresses. It uses a smart contract that accepts ETH deposits that can be withdrawn by a different address. To preserve privacy a relayer can be used to withdraw to an address with no ETH balance. Whenever ETH is withdrawn by the new address, there is no way to link the withdrawal to the deposit, ensuring complete privacy.

– Tornado Cash

But blockchain analysis is not just the domain of government and law enforcement, or the criminals seeking to evade them. It can also be leveraged to provide insights into the health and overall functioning of all blockchain-based platforms. Crypto is a unique industry, as actions and transactions are not reported quarterly, if at all – like in traditional finance and commerce – but rather in real-time.

Tools such as Skynet utilize this real-time data to provide actionable security insights. Analyzing metrics such as the number of transactions interacting with a protocol, the number of discrete users, and the number of events emitted by a protocol can provide a wealth of information that paints a specific picture of a platform's functioning over time. Individual traders and investors can make use of these tools to monitor platforms and projects in which they have invested.

DeFi users can also utilize several different platforms that monitor their wallets – or anyone else's wallet – and send an alert whenever a transaction is processed. This allows them to have real-time notifications about any activity on the addresses most important to them, whether it's final confirmation of a low-priority transaction broadcast to the network hours before, or the first attempt of a hacker to gain control of or drain funds from their account.

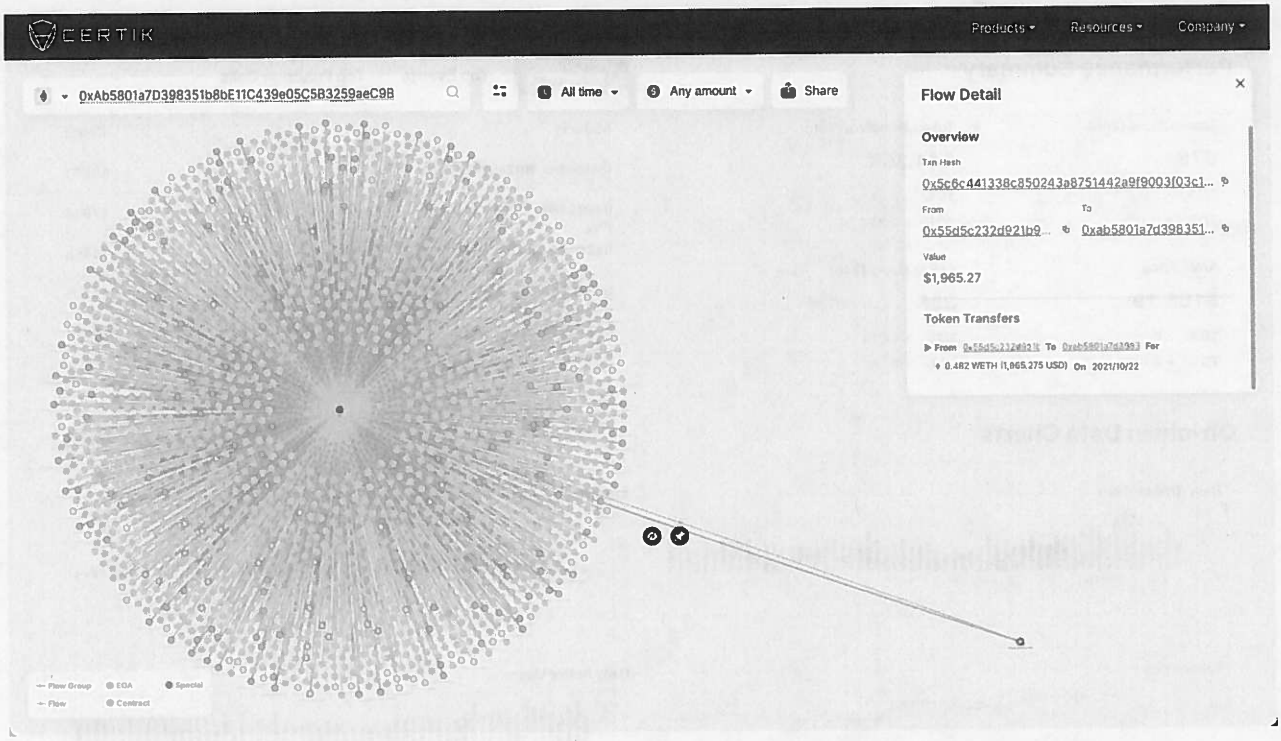
Blockchain analysis is a rich and continuously expanding field. Now that we've gone over what blockchain analysis is, let's take a look at the tools that are available to help you leverage it in your research and how exactly these tools work.

What Blockchain Analysis Tools are Available?

Etherscan is likely to be the tool that DeFi users are most familiar with. Many DeFi platforms provide a direct link to the website after every transaction, so the user can check on its confirmation status. Etherscan is an excellent tool for confirming transactions and getting a general overview of a particular wallet's holdings. Additionally, the fact that the site tags many well known wallets (e.g. Coinbase 1 Hot Wallet or Uniswap V3 Router) makes it relatively easy to see at a glance where your money is coming from and going.

Etherscan is great for raw data such as wallet balances and transaction history; the who, what, and how much. But if you're looking for second-level insights, you'll need to turn to a tool that aggregates and analyzes this raw data.

Skytrace is a blockchain analysis tool that greatly simplifies the process of tracing the flow of funds from one wallet to another. Skytrace visualizes a wallet's interactions with other addresses and has helpful tags for well-known protocols, such as Uniswap and Tornado Cash.



Using Skytrace to visualize one of Vitalik Buterin's hundreds of transactions, in this case his sale of 6,757.307 HEX for 0.48 ETH on Uniswap

CertiK's Skynet combines six security primitives to arrive at a comprehensive score that reflects the effectiveness of a DeFi project's security measures. These six primitives are: social sentiment, on-chain monitoring, governance, market dynamics, safety analysis, and finally the Security Oracle. With the exception of the social sentiment metric, each of these primitives incorporate blockchain analysis.

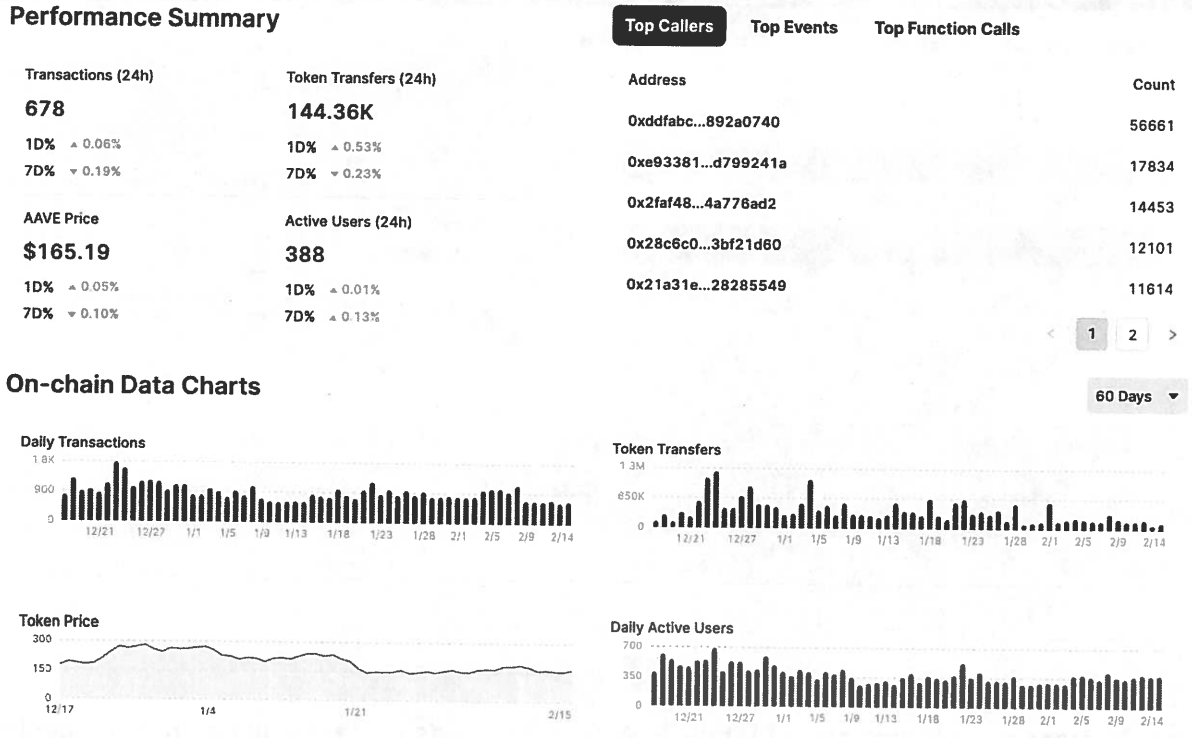
Breaking down each of these primitives will provide illustrative case studies of how blockchain analysis works.

How Does Blockchain Analysis Work?

Blockchain analysis works by aggregating the massive amount of data that blockchains produce, and then filtering, modeling, or otherwise inspecting it in order to produce actionable insights. These insights could be anything from a transaction linking two wallets, an important wallet making moves before or after big announcements, or a gradual decay in the number of active users of a specific DeFi protocol.

That's the short answer. To really understand how blockchain analysis works, let's take a deep dive into a specific example of on-chain monitoring. Skynet is CertiK's security scoring tool that uses on-chain analysis to arrive at actionable security and data insights.

On-chain Monitoring



AAVE's entry on the Security Leaderboard. The tab shown is Skynet's on-chain monitoring analysis

The on-chain monitoring section of the Security Leaderboard gives a comprehensive overview of a project's activity. You can see the number of transactions interacting with the protocol over the last 24 hours, the number of transfers of the project's token, the number of active users, and the price of the token, plus all of these metrics plotted over a customizable period.

The next Skynet primitive is Governance. Decentralized governance is one of the most important factors that put the De in DeFi. Decentralized protocols have governance forums where users can propose, debate, and vote on ideas in an open, collaborative process. Any protocol that is governed in such a way is a DAO – a Decentralized Autonomous Organization. As you can imagine, when the power to make any and all decisions lies with a DAO, it's important for investors to pay close attention to the votes and actions it undertakes (if they're not getting directly involved themselves).

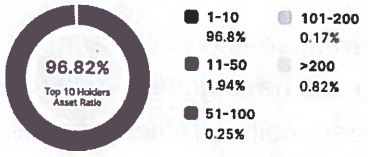
Governance & Autonomy

Token Holder Distribution Analysis

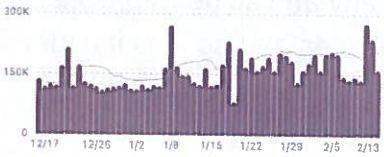
Total Holders: 1,620,281

50% Token Supply: 1 Holder

Holder Asset Distribution



Daily New Users (30 days)



Top 100 Token Holders

	Address	Percentage	Quantity	Value
1	Burn Address	58.1787%	372,689,180	$3,067,373,217
2	PancakeSwap: Main ...	33.5618%	214,994,849	$1,769,489,097
3	Pancake LPs (Cake-L...	2.3481%	15,041,476	$123,797,046
4	Exchange Wallet	1.5129%	9,691,501	$79,764,730
5	Exchange Wallet	0.3076%	1,970,266	$16,216,032
6	PancakeSwap: SYRU...	0.2434%	1,559,033	$12,831,430
7	0x8076...b8d7d7	0.1794%	1,149,491	$9,460,749
8	0x5a52...70efcb	0.1789%	1,145,956	$9,431,655
9	PancakePair	0.1553%	994,702	$8,186,771
10	0xaaf4...e1de82	0.1542%	987,865	$8,130,507

< 1 2 3 4 5 ... 10 >

Privileged Transactions | Privileged Addresses | Privileged Functions

Tx Hash	Caller	Contract	Function	Timestamp
0xfdc2...6446a4	0x0f93...7a3373 Deployer	0x0...e82	transfer	300d ago
0x4fc0...92eae6	0x0f93...7a3373 Deployer	0xb...812	setFeeToSetter	303d ago
0x0261...c90b3c	0x0f93...7a3373 Deployer	0xb...812	setFeeTo	303d ago
0x8cf0...cc83a4	0x0f93...7a3373 Deployer	0xb...812	createPair	354d ago
0xd701...55df78	0x0f93...7a3373 Deployer	0xb...812	createPair	356d ago

< 1 2 3 4 5 ... 8 >

PancakeSwap's Skynet Governance Module

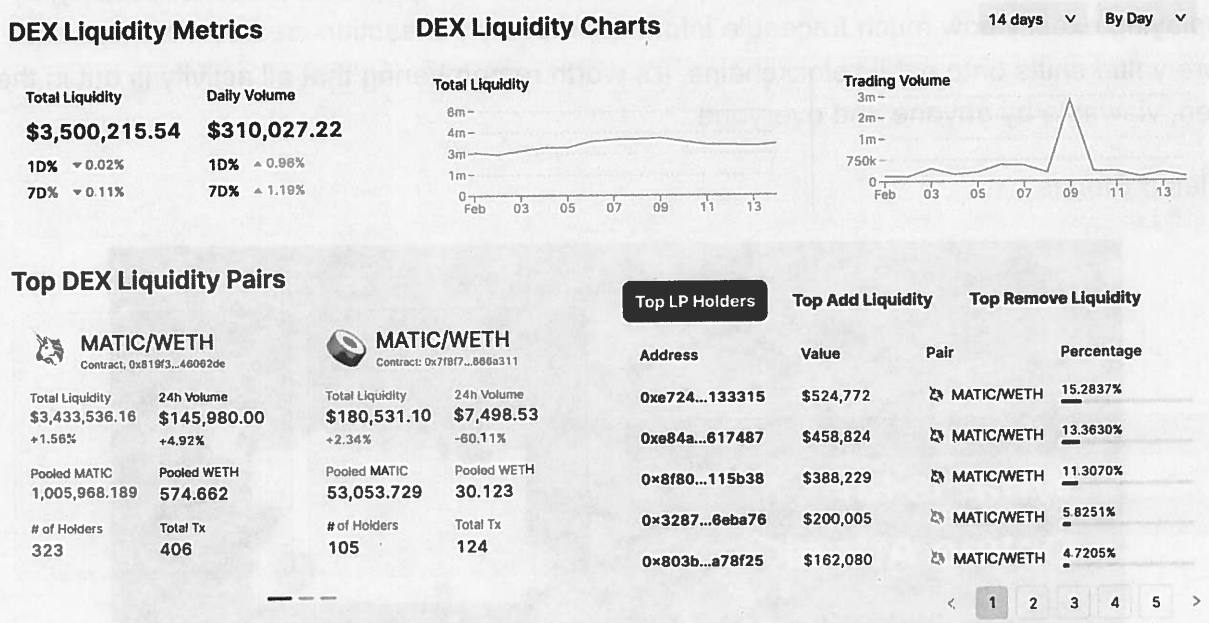
The Governance Score is an overall rating of the platform's decentralization, links to major crypto platforms, and the health of its DAO. The on-chain component of Skynet's Governance score is made up of the following metrics.

Privileged Transactions lists the number of privileged transactions in the last 72 hours. A privileged transaction is one initiated by an address that has power to modify a platform's smart contracts. A truly decentralized DeFi protocol should only be able to be updated or changed after its DAO has voted on and approved the changes. Recent Privileged Transactions is similar, but here we get a list of all privileged transactions, not just in the last 72 hours. It's a great way to see how often a platform's smart contracts are modified, by whom, and for what purpose.

The Privileged Addresses section lists all the addresses that have the power to initiate privileged transactions (as defined above). You can click on the address or contract to be taken to its listing on a block explorer – BSCScan in this case, since PancakeSwap runs on Binance Smart Chain.

Privileged Functions outlines the code functions that privileged addresses can invoke. In this case we've got burn, constructor, and mint. The burn function sends tokens to an address where they cannot be retrieved. The constructor function is called when initializing a contract. It sets the contract's variables to the correct state. Mint creates new tokens, often for liquidity mining rewards.

Market Volatility



Matic's entry on the Security Leaderboard

Decentralized exchanges (DEXs) function entirely on-chain, which means all the data they create is freely available. This is great news for anyone seeking to do research on decentralized market dynamics.

Skynet analyzes this data to provide actionable insights. At a single glance, you can see exactly which token pairs have the deepest liquidity, volume plotted over time, and the largest holders of liquidity provider (LP) tokens. All this data helps give an accurate overview of the health of a particular token's market dynamics. For example, if you see in the Top Remove Liquidity tab that all of the major LP Holders are suddenly withdrawing their positions, you may take that as a reason to do some further investigation.

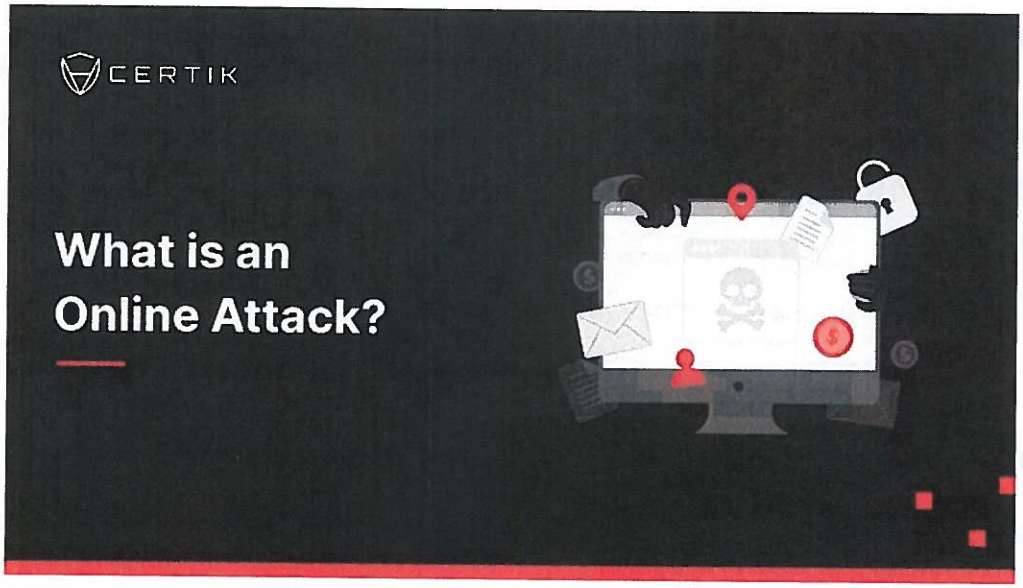
Blockchain Analysis – An Increasingly Powerful Tool

With the consistent growth of blockchain adoption and the data that users, platforms, and miners produce, blockchain analysis becomes more powerful every day. Larger datasets mean deeper insights. With the approaching Web3 economy focused on using blockchain technology to empower everyone left out of centralized Web2 platforms, blockchains are the newest frontier of data analysis.

Powerful tools exist to help all blockchain users gain insights into Web3 platforms. CertiK's Skynet is a security-focused resource that demystifies the complex technicalities of DeFi security, while Skytrace makes it easy to perform your own blockchain data analysis and map out interactions between wallets visually.

Blockchain analysis is a uniquely insightful way to understand the functioning and security of blockchain platforms. But it can also help you take control of your own personal security, by displaying exactly how much traceable information every transaction creates. As more and more value shifts onto public blockchains, it's worth remembering that all activity is out in the open, viewable by anyone and everyone.

Related Stories

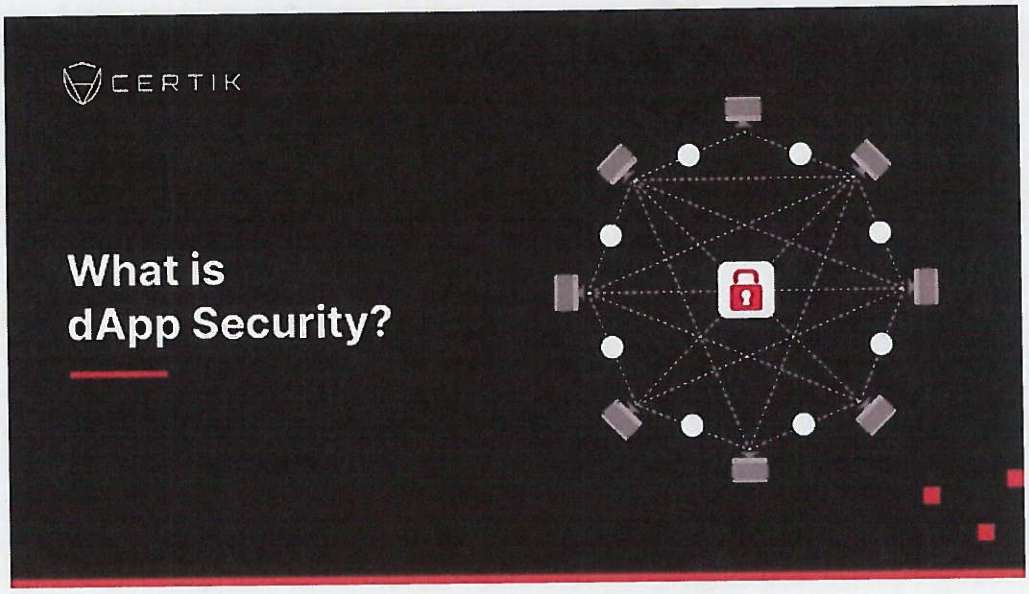


Blogs

What is an Online Attack?

One of the promises of blockchain technology is its ability to bolster the safety of online activity through the greater security afforded by decentralization. However, despite this added security, it is naive to assume that online attacks will just go away. With that in mind, this post provides an overview of some of the most infamous online attacks, how they intersect with blockchain technology, and some of the ways of defending against such attacks.

5/8/2022

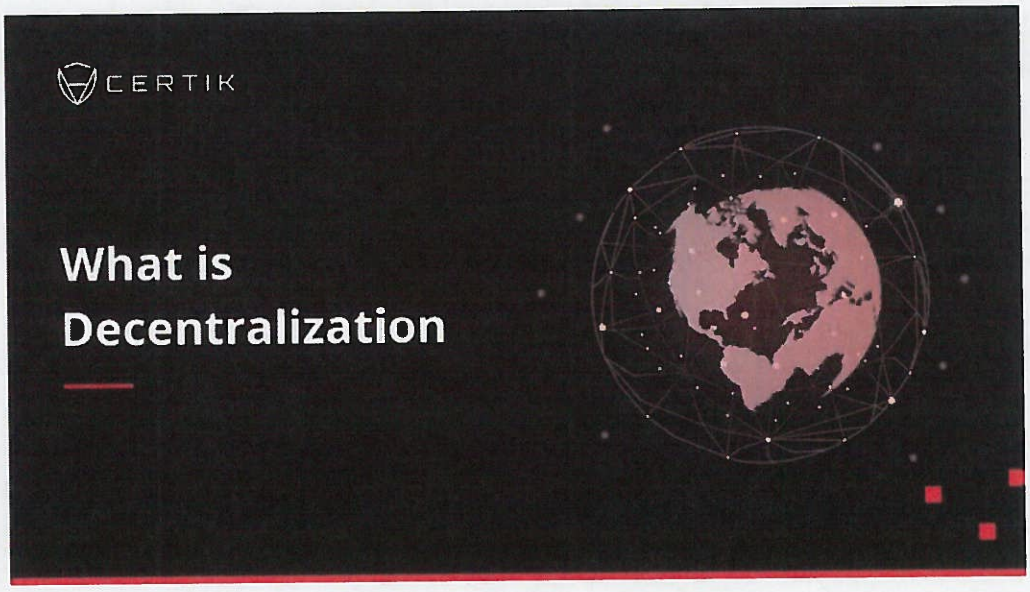


Blogs

What is dApp Security?

The systematic set up of decentralized apps unfortunately leaves them susceptible to hackers in some situations. As more businesses migrate to dApps and other cloud-based structures, it is important to keep safety and security in mind. Even as technology changes, cybercriminals will look for ways to infiltrate it.

4/8/2022



Blogs

What is Decentralization?

EXHIBIT 110

Backgrounder

Cryptocurrencies, Digital Dollars, and the Future of Money

The dizzying rise of Bitcoin and other cryptocurrencies has created new challenges for governments and central banks. Some are responding by introducing their own digital currencies.

WRITTEN BY
Anshu Siripurapu

UPDATED
Last updated September 24, 2021 12:55 pm (EST)

Summary

Since the creation of Bitcoin in 2009, cryptocurrencies have exploded in popularity and are today collectively worth trillions of dollars.

Although they can offer benefits to consumers and investors, they can also be leveraged by bad actors and pose economic risks.

In response, many governments are considering introducing their own digital currencies.

Introduction

In the span of a few years, cryptocurrencies have grown from digital novelties to trillion-dollar technologies with the potential to disrupt the global financial system. Bitcoin and hundreds of other cryptocurrencies are increasingly held as investments, and they are used to buy everything from software to real estate to illegal drugs.

To proponents, cryptocurrencies are a democratizing force, wresting the power of money creation and control from central banks and Wall Street. Critics, however, say the new technology is wildly unregulated and is empowering criminal groups, terrorist organizations, and rogue states. Electricity-guzzling crypto mining is also harmful to the environment, they argue.

Financial regulators are now scrambling to respond. Regulations vary considerably around the world, with some governments embracing cryptocurrencies and others banning or limiting their use. Central banks around the world, including the U.S. Federal Reserve, are considering introducing their own digital currencies to compete with the crypto boom.

What are cryptocurrencies?

So called for their use of cryptography principles to mint virtual coins, cryptocurrencies are typically exchanged on decentralized computer networks between people with virtual wallets. These transactions are recorded publicly on distributed, tamper-proof ledgers known as blockchains. This open-source framework prevents coins from being duplicated and eliminates the need for a central authority such as a bank to validate transactions. Bitcoin, created in 2009 by the pseudonymous software engineer Satoshi Nakamoto, is by far the most prominent cryptocurrency, and its total value has at times exceeded $1 trillion. But numerous others, including Ethereum, the second-most popular, have proliferated in recent years and operate on the same general principles.

Full URL: https://www.cfr.org/backgrounder/cryptocurrencies-digital-dollars-and-future-money?gclid=EAIaIQobChMI-b_uvai6-gIVk4vICh1BLAqHEAAYASAAEgLz%E2%80%A6

Cryptocurrency users send funds between digital wallet addresses. These transactions are then recorded into "blocks," and confirmed across the network. Blockchains do not record real names or physical addresses, only the transfers between digital wallets, and thus confers a degree of anonymity on users. Some cryptocurrencies, such as Monero, claim to provide additional privacy. However, if the identity of a wallet owner becomes known, their transactions can be traced.

Bitcoin "miners" earn coins by validating transactions on the network, a process that requires them to solve mathematical problems using computers to guess and check trillions of possible solutions, known as "proof of work." Many cryptocurrencies use this method, but some instead use a validation mechanism known as "proof of stake." In Bitcoin's case, a transaction block is added to the chain every ten minutes, at which point new Bitcoin is awarded. (The reward decreases steadily over time.) The total supply of Bitcoin is capped at twenty-one million coins, but not all cryptocurrencies have such a constraint.

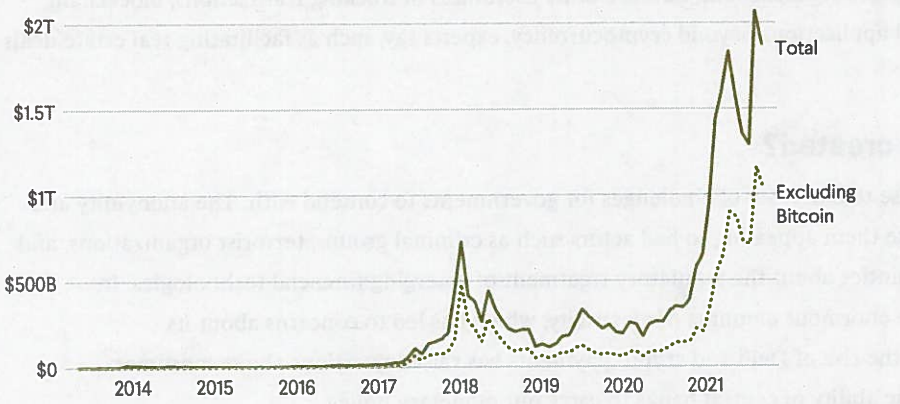
The prices of Bitcoin and many other cryptocurrencies vary based on global supply and demand. However, the values of some cryptocurrencies are fixed because they are backed by other assets, thus earning them the name "stablecoins." For example, the value of the popular stablecoins Tether and USD Coin is purportedly pegged at $1 per coin, though authorities have alleged this is not always the case.

Why are they popular?

Once dismissed as a fringe interest of tech evangelists, cryptocurrencies—particularly Bitcoin—have skyrocketed in value in recent years. In 2021, the price of a Bitcoin surged to more than $60,000 for the first time. Different currencies have different appeals, but the popularity of cryptocurrencies largely stems from their decentralized nature: They can be transferred relatively quickly and anonymously, even across borders, without the need for a bank that could block the transaction or charge a fee. Dissidents in authoritarian countries have raised funds in Bitcoin to circumvent state controls, for example. Some experts say that digital assets are primarily tools for investment.

Cryptocurrencies Have Exploded in Value in Recent Years

Market value of all crypto assets



Source: CoinMarketCap.com.

The price of Bitcoin and other cryptocurrencies fluctuates wildly, and some experts say this limits their usefulness as a means of transaction. (Most buyers and sellers don't want to accept payment in something whose value can change dramatically from day to day.) Nevertheless, some businesses accept Bitcoin. Many investors see Bitcoin as a speculative asset to hold over time, rather than make payments with, and it often draws comparisons to gold. Some see Bitcoin as a hedge against inflation because the supply is permanently fixed unlike those of fiat currencies, which central banks can expand indefinitely. However, some experts have questioned this argument. The valuation of other cryptocurrencies can be harder to explain; for instance, Dogecoin was created as a joke yet has surged in price, partly due to the support of some high-profile investors and entrepreneurs.

In countries with historically weak currencies, including several Latin American and African countries, Bitcoin has become popular with citizens. In 2021, El Salvador made waves by becoming the first country to make Bitcoin legal tender (residents can pay taxes and settle debts with it), though the move has sparked protests. Some politicians in other parts of the region have expressed support for the idea.

Stablecoins, meanwhile, have the potential to rival fiat currencies as the dominant form of payments, experts say. Their value is relatively stable, and they can be sent instantly without the transaction fees associated with credit cards or international remittance services such as Western Union. In addition, because stablecoins can be used by anyone with a smartphone, they represent an opportunity to bring millions of people who lack traditional bank accounts into the financial system. "Stablecoins are very promising as a form of low-cost, high-speed, inclusive payment technology," says CFR's Brent McIntosh.

What is "DeFi"?

Cryptocurrencies and blockchains have given rise to a new constellation of "decentralized finance" or DeFi businesses and projects. Essentially the cryptocurrency version of Wall Street, DeFi aims to offer people access to financial services —borrowing, lending, and trading—without the need for legacy institutions such as banks and brokerages, which often take large commissions and other fees. Instead, "smart contracts" automatically execute transactions when certain conditions are met. DeFi is surging in popularity, with investors pouring tens of billions of dollars into the sector.

Most DeFi apps are built on the Ethereum blockchain. Because of its usefulness in tracking transactions, blockchain technology has a range of potential applications beyond cryptocurrency, experts say, such as facilitating real estate deals and international trade [PDF].

What challenges has this created?

Cryptocurrencies have also given rise to a new set of challenges for governments to contend with. The anonymity and portability of cryptocurrencies make them appealing to bad actors such as criminal groups, terrorist organizations, and rogue states. There are also uncertainties about the regulatory treatment of emerging financial technologies. In addition, crypto mining can require enormous amounts of electricity, which has led to concerns about its environmental effects. Meanwhile, the rise of DeFi and crypto payments has raised questions about consumer protection, market volatility, and the ability of central banks to carry out monetary policy.

Illicit activities. In recent years, cybercriminals have increasingly carried out ransomware attacks, by which they infiltrate and shut down computer networks and then demand payment to restore them, often in cryptocurrency. Drug cartels and money launderers are also "increasingly incorporating virtual currency" into their activities, according to

the U.S. Drug Enforcement Agency's (DEA) most recent annual assessment. U.S. and European authorities have shut down a number of so-called darknet markets—websites where anonymous individuals can use cryptocurrency to buy and sell illegal goods and services, primarily narcotics.

Terrorism and sanctions evasion. The primacy of the U.S. dollar has provided the United States unrivaled power to impose crippling economic sanctions. However, sanctioned states including Iran and North Korea are increasingly using cryptocurrency to evade U.S. penalties. Meanwhile, terrorist groups such as the self-proclaimed Islamic State, al-Qaeda, and the military wing of the Palestinian organization Hamas also traffic in crypto.

Environmental harms. Bitcoin mining is an enormously energy-intensive process: the network now consumes more electricity than many countries. This has sparked fears about crypto's contributions to climate change. Cryptocurrency proponents say this problem can be solved using renewable energy; El Salvador's president has pledged to use volcanic energy to mine Bitcoin, for example. Environmental concerns reportedly prompted Ethereum's move to a proof-of-stake model, which uses less energy.

Unregulated finance. The rapid rise of cryptocurrencies and DeFi enterprises means that billions of dollars in transactions are now taking place in a relatively unregulated sector, raising concerns about fraud, tax evasion, and cybersecurity, as well as broader financial stability. If cryptocurrencies become a dominant form of global payments, they could limit the ability of central banks, particularly those in smaller countries, to set monetary policy through control of the money supply.

What are governments doing about this?

Many governments initially took a hands-off approach to cryptocurrencies, but their rapid ascent and evolution, coupled with the rise of DeFi, has forced regulators to begin crafting rules for the emerging sector, a process that could take years. Regulations vary widely around the world, with some governments embracing cryptocurrencies and others banning them outright. The challenge for regulators, experts say, is to develop rules that limit traditional financial risks without stifling innovation.

Most Governments Have Permitted Cryptocurrencies

Regulation of cryptocurrencies as of June 2021, selected countries

Sources: Thomson Reuters Regulatory Intelligence; CFR research.

COUNCIL on FOREIGN RELATIONS

In the United States, policymakers have indicated they are moving to regulate cryptocurrencies and the emerging DeFi sector. However, cryptocurrencies do not fit neatly into the existing regulatory framework, creating ambiguity that lawmakers will likely have to resolve. U.S. Securities and Exchange Commission (SEC) Chairman Gary Gensler has called the cryptocurrency sector a "Wild West," and urged Congress to give the SEC greater powers. Federal Reserve Chairman Jerome Powell and Treasury Secretary Janet Yellen have both called for stronger regulations of stablecoins.

To limit illicit activities, authorities have targeted the exchanges that allow users to convert cryptocurrencies to U.S. dollars and other national currencies. Under pressure from regulators, major exchanges including Coinbase, Binance, and Gemini adhere to "know your customer" and other anti–money laundering requirements. Law enforcement and intelligence agencies, meanwhile, have learned to leverage the traceability of most cryptocurrencies by using blockchains to analyze and track criminal activity. For example, some of the ransom paid to the Colonial Pipeline hackers was later recovered by the FBI. In September 2021, the Treasury Department announced a crackdown on the use of cryptocurrencies in ransomware attacks, issuing its first sanctions on a crypto exchange.

China, which accounts for most of the world's Bitcoin mining, has moved aggressively to crack down on cryptocurrencies. In September 2021, Chinese authorities announced a sweeping ban on all crypto transactions and mining, causing the price of some cryptocurrencies to fall sharply in the immediate aftermath. A handful of other countries, including Bolivia, Nigeria, and Russia, have also moved to limit the use of crypto, and others are considering restrictions. Still, most governments have so far taken a relatively limited approach.

What is a central bank digital currency?

In an effort to assert sovereignty, many central banks, including the U.S. Federal Reserve, are considering introducing their own digital cash, known as central bank digital currency (CBDC). For proponents, CBDC promises the speed and other benefits of cryptocurrency without the associated risks. Dozens of countries—together representing more than 90 percent of the global economy—are exploring CBDC. China is moving ahead quickly: it piloted a digital yuan in late 2019 that is now used for billions of dollars of transactions. In the United States, there is reportedly disagreement among Fed officials over the need for a digital dollar.

Experts say interest in CBDC intensified in 2019 when Facebook announced it would create its own digital currency called Libra, potentially offering a new payment option for its more than two billion users. (The company has since scaled back the project, renamed Diem.) China is another motivating factor: A digital yuan could give Beijing even more control over its economy and citizens, and threaten the U.S. dollar's status as the favored international reserve currency, experts say.

One way to implement CBDC would be for citizens to have accounts directly with the central bank [PDF]. This would give governments powerful new ways of managing the economy—stimulus payments and other benefits could be credited to people directly, for example—and the central bank's imprimatur would make CBDC a safe digital asset to hold. But their introduction could also create new problems, CFR's McIntosh and other experts say, by centralizing an enormous amount of power, data, and risk within a single bank and potentially compromising privacy and cybersecurity.

Some experts say the potential for CBDC to cut out commercial banks as intermediaries carries risks, because these banks perform a critical economic role by creating and allocating credit (i.e., making loans). If people chose to bank directly with the Fed, that would require the central bank to either facilitate consumer borrowing, which it might not

be equipped to do, or find new ways of injecting credit. For these reasons, some experts say private, regulated digital currencies are preferable to CBDC.

Recommended Resources

In this 2008 paper [PDF], pseudonymous engineer Satoshi Nakomoto proposes Bitcoin, the first cryptocurrency.

In this free Massachusetts Institute of Technology class, SEC Chair Gary Gensler explores Bitcoin, blockchains, and money.

The *Economist* examines the potential benefits and risks of DeFi.

At this CFR virtual meeting, experts discuss the prospects for central bank digital currencies.

In this August 2021 speech, Federal Reserve Governor Christopher J. Waller questions the need for a digital dollar.

Ankit Panda contributed to this report.

For media inquiries on this topic, please reach out to communications@cfr.org.

EXHIBIT 116

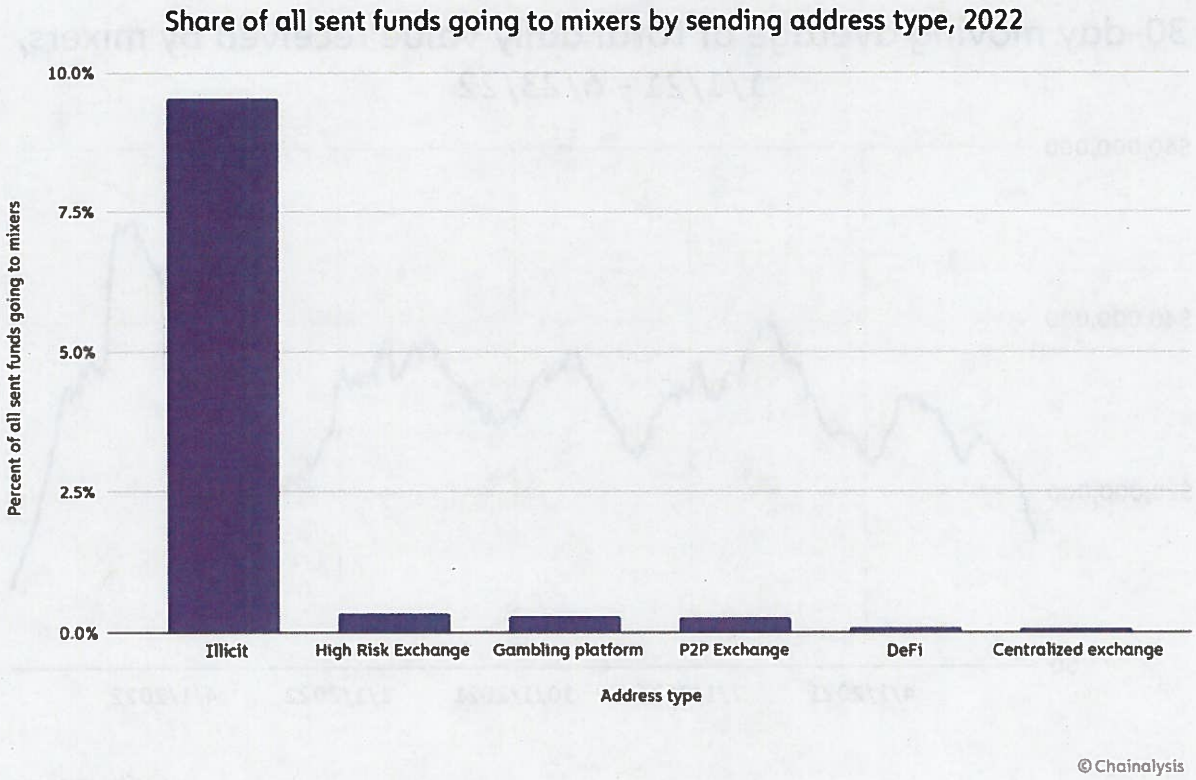
Crypto Mixer Usage Reaches All-time Highs in 2022, With Nation State Actors and Cybercriminals Contributing Significant Volume

blog.chainalysis.com/reports/crypto-mixer-criminal-volume-2022/

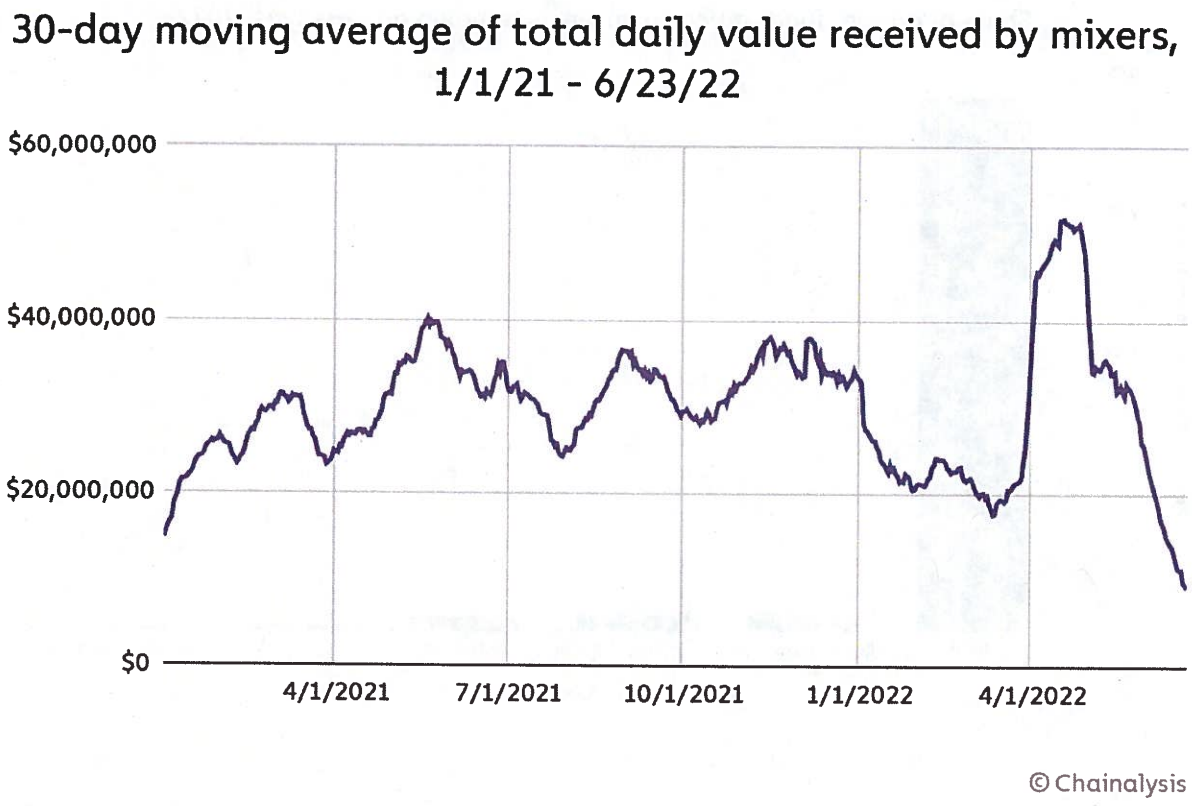
Chainalysis Team

July 14, 2022

Crypto mixers are a go-to tool for cybercriminals on the blockchain. We find that in 2022, crypto addresses tied to illicit activity transferred nearly 10% of their funds to mixers – with no other address type sending more than 0.3%.



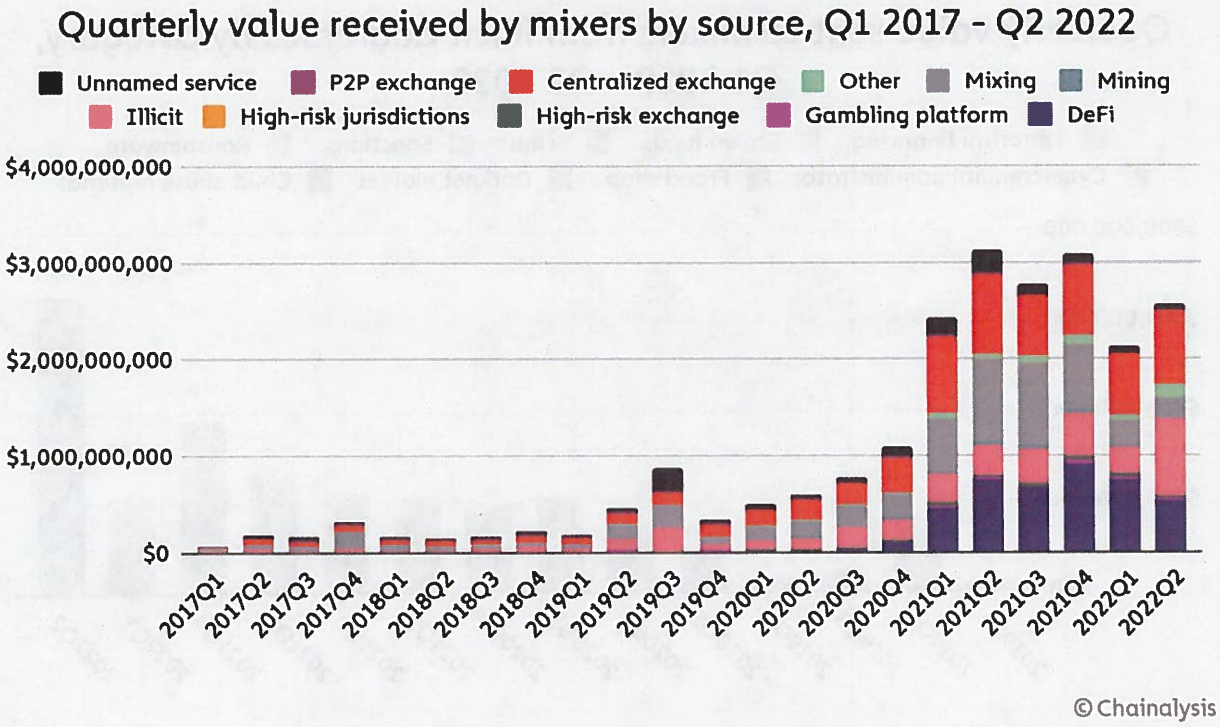
Crypto mixers may soon become obsolete as Chainalysis refines its ability to demix transactions, but for the time being, our data shows that mixers are processing more cryptocurrency than ever. On April 19, 2022, the 30-day moving average value received by mixers reached an all-time high of $51.8 million worth of cryptocurrency — double the value received by mixers at the same time in 2021.



Below, we'll dive into who's driving the increase in mixer usage and what it means for law enforcement and compliance pros.

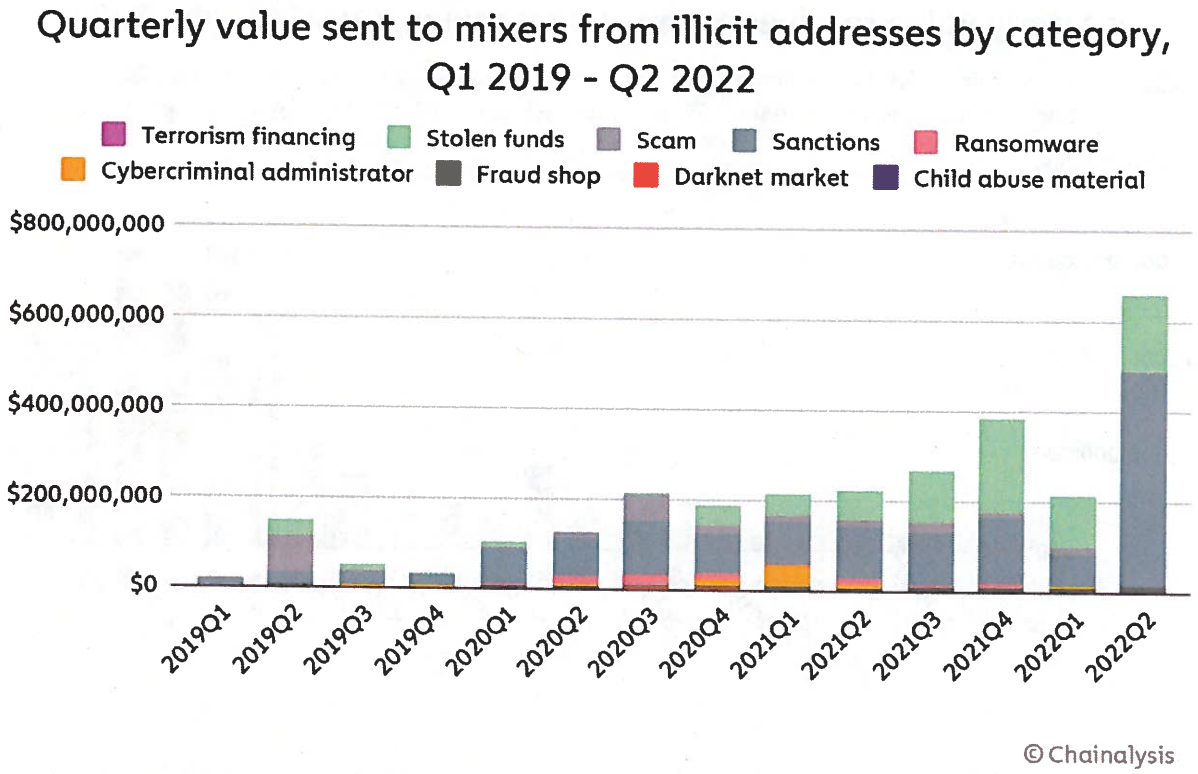
What's driving the increase in mixer usage?

Cryptocurrency mixers saw significant quarter-over-quarter volume increases starting in 2020 and continuing through 2021. While that growth has leveled off somewhat this year, it remains close to all-time highs.



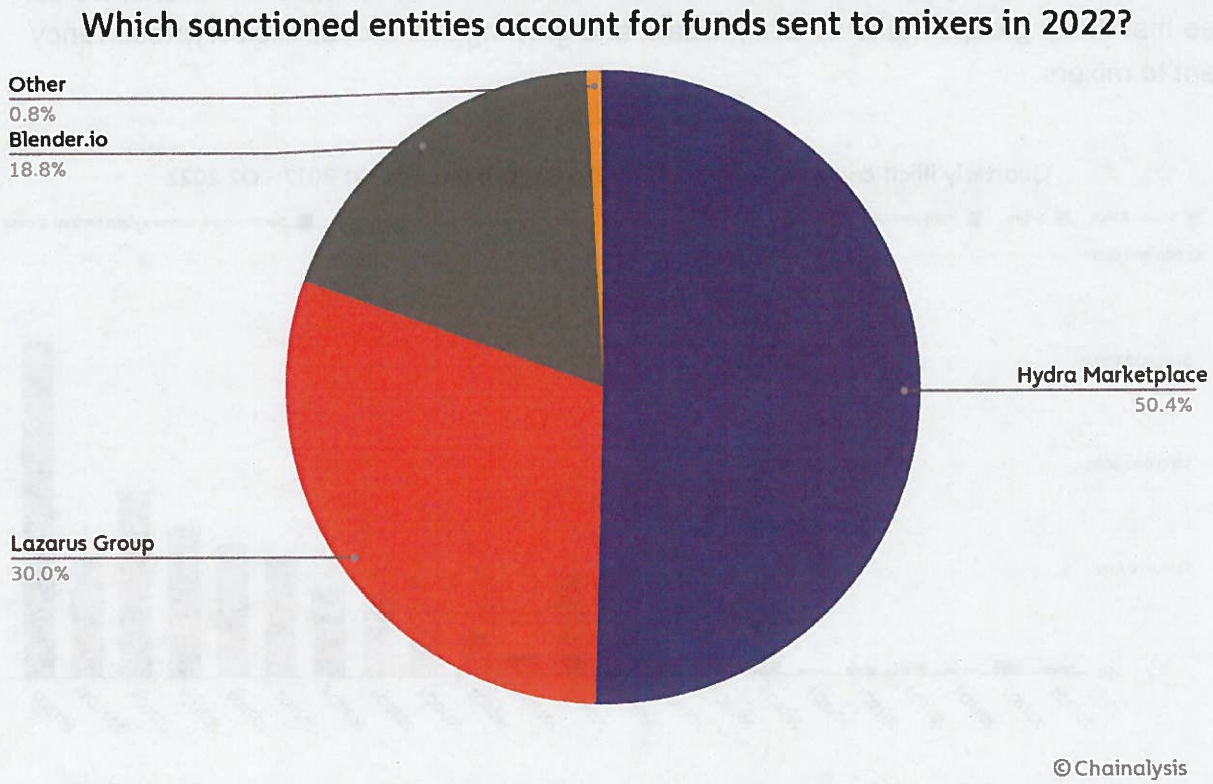
The increases come primarily from growth in the volume sent from centralized exchanges, DeFi protocols, and most notably, addresses connected to illicit activity. DeFi protocols in particular have risen not just in terms of value sent to mixers, but also in terms of the share of all volume sent to mixers, which makes sense given that the timing coincides with DeFi's increasing prominence within the overall cryptocurrency ecosystem.

The increase in illicit cryptocurrency moving to mixers is more interesting though. Illicit addresses account for 23% of funds sent to mixers so far in 2022, up from 12% in 2021. On the chart below, we examine the types of criminal activity those illicit actors are associated with.



Note: Sanctioned entities on the graph above includes volume sent from entities that, prior to being sanctioned, would have fit in another category. For example, Hydra Market is a darknet market that was sanctioned in Q1 2022 – all of its volume from previous years is now labeled as "Sanctions."

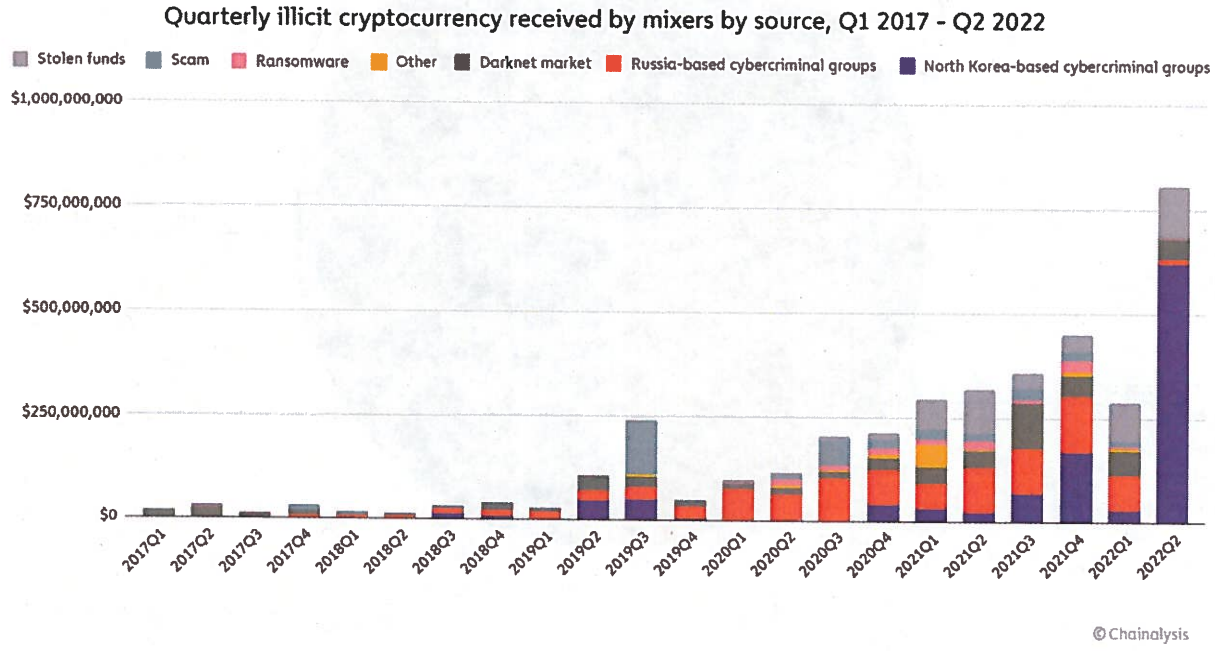
What stands out most is the huge volume of funds moving to mixers from addresses associated with sanctioned entities, especially in Q2 2022. Below, we look at which specific sanctioned entities have accounted for those funds so far in 2022.



Russian darknet market Hydra, which was sanctioned in April 2022, leads the way here, accounting for 50% of all funds moving to mixers from sanctioned entities this year. Importantly, drug sales weren't the only reason OFAC decided to go after Hydra. DOJ officials specified that Hydra played a role in laundering funds from other darknet markets, cryptocurrency thefts, and ransomware attacks — the market offered mixer-like services of its own — and facilitated the sale of stolen data and hacking tools used in cyber attacks. Given the outsized role that Russia plays in cybercrime, and the connections some of these cybercriminal groups have to Russian intelligence services, an increase in funds moving from services like Hydra to mixers could be significant from a national security standpoint.

Nearly all of the remaining funds moving from sanctioned entities to mixers come from two groups associated with the North Korean government: Lazarus Group and Blender.io. Lazarus Group is a cybercrime syndicate responsible for several cryptocurrency hacks on behalf of the North Korean government, and along with associated groups remains extremely active today. Already in 2022, hackers associated with the North Korean government are believed to have stolen over $1 billion worth of cryptocurrency, mostly from DeFi protocols. Blender.io, on the other hand, became the first ever mixer sanctioned this year for its role in laundering funds stolen by Lazarus Group and others associated with North Korea. Any funds it sends to other mixers could very well represent a continuation of that illegal activity.

Overall, if we label cybercriminal organizations with known nation state affiliations, we can see that these groups make up a significant and growing share of all illicit cryptocurrency sent to mixers.



Note: Transaction volume has no known nation state connection unless otherwise noted

Funds sent to mixers by cybercriminal groups associated with Russia, and especially those associated with North Korea, have risen dramatically in 2021 and 2022.

Balancing privacy with safety

Crypto mixers present a difficult dilemma to regulators and members of the cryptocurrency community. Virtually everyone would acknowledge that privacy is valuable, and that in a vacuum, there's no reason services like mixers shouldn't be able to provide it. But the data suggest that 25% of mixed funds come from illicit addresses, and that cybercriminals associated with hostile governments are among those taking the most advantage.

We encourage stakeholders in the public and private sectors to work together on how to address the risks associated with mixers, and stand ready to provide any data necessary to make those engagements as productive as possible.

This material is for informational purposes only, and is not intended to provide legal, tax, financial, or investment advice. Recipients should consult their own advisors before making these types of decisions. Chainalysis has no responsibility or liability for any decision made or any other acts or omissions in connection with Recipient's use of this material.

Chainalysis does not guarantee or warrant the accuracy, completeness, timeliness, suitability or validity of the information in this report and will not be responsible for any claim attributable to errors, omissions, or other inaccuracies of any part of such material.

EXHIBIT 120

Introduction to Tornado Cash

Tornado Cash is a **fully decentralized non-custodial protocol** allowing private transactions in the crypto-space.

As a decentralized protocol, Tornado.Cash smart contracts have been implemented within the Ethereum blockchain, making them immutable. They can neither be changed nor tampered with. Therefore, nobody - including the original developers - can modify or shut them down. All governance and mining smart contracts are deployed by the community in a decentralized manner.

As a non-custodial protocol, users keep custody of their cryptocurrencies while operating Tornado.Cash. This means that at each deposit, they are provided with the private key enabling the access to the deposited funds, which gives users complete control over their assets.

How is privacy achieved?

Tornado Cash improves transaction privacy by breaking the on-chain link between source and destination addresses. It uses a smart contract that accepts ETH & other tokens deposits from one address and enables their withdrawal from a different address.

To maximize privacy, several steps are recommended, such as the use of a relayer for gas payments to withdraw funds from an address with no pre-existing balance.

More details are available in *Behind the scenes: How does Tornado.Cash work?* & Tips to remain

anonymous.

Where does Tornado.cash operate?

Since its inception in 2019, Tornado Cash has been operating **on the Ethereum blockchain**. The protocol has been offering diversified fixed amount pools for six tokens (ETH, DAI, cDAI, USDC, USDT & WBTC) handled by the Ethereum blockchain.

Since June 2021, in addition to the Ethereum blockchain, Tornado Cash smart contracts **have also been deployed on other side-chains & blockchains**. These deployments enabled the tool to either support new tokens or benefit from Layer-2 advantages, such as faster and cheaper transactions.

As of today, Tornado Cash is operating on:

- **Ethereum Blockchain** : **ETH** (Ethereum), **DAI** (Dai), **cDAI** (Compound Dai), **USDC** (USD Coin), **USDT** (Tether) & **WBTC** (Wrapped Bitcoin),
- **Binance Smart Chain**: **BNB** (Binance Coin),
- **Polygon Network**: **MATIC** (Polygon),
- **Gnosis Chain (former xDAI Chain)**: **xDAI** (xDai),
- **Avalanche Mainnet**: **AVAX** (Avalanche),
- **Optimism**, as a Layer-2 for **ETH** (Ethereum),
- **Arbitrum One**, as a Layer-2 **ETH** (Ethereum).

Until December 2021, the protocol included an anonymity mining system for some of these tokens, allowing its users to earn a governance token (**TORN**). Users were able to ultimately earn TORN on the Blockchain network by depositing in the ETH, DAI, cDAI & WBTC pools.

More information on Anonymity mining & Tornado.Cash token is available.

Thanks to the TORN token, Tornado Cash users can actively participate in shaping the protocol. The community has a strong weight regarding the evolution of Tornado Cash and the improvement of its features. Indeed, protocol parameters & token distribution are completely under the community's control through this governance.

All pools mentioned above can be accessed on tornadocash.eth.link. They operate **under the principle of fixed-amount deposits & withdrawals**. It means that each token has 2 to 4 different pools, allowing transactions of only 2 to 4 different fixed amounts *(e.g. ETH has four different pools, one for each of these amounts: 0.1, 1, 10 & 100 ETH)*.

Tornado Cash Nova

With the **release of Tornado Cash Nova** (beta version) on December 2021, an **upgraded pool with unique new features** has been added to the protocol. Users are no longer constrained by fixed-amount transactions. With the addition of Tornado Cash Nova, they can benefit from the use of **an arbitrary amount pool & shielded transfers**.

Tornado Cash Nova operates on the Gnosis Chain (former xDai Chain) as a Layer2 to optimize speed and cost. It allows **deposits and withdrawals of completely customized amounts in ETH**. This pool also enables shielded transactions where users can **transfer the custody of their token while remaining in the pool**.

Tornado Cash Nova (beta version) can be accessed on nova.tornadocash.eth.link. You can find further informations related to the functioning of Tornado Cash Nova in the dedicated section of our docs.

How does Tornado.Cash run?

Codes behind Tornado.Cash functioning - smart contacts, circuits & toolchain - are fully **open-**

sourced. Working as a DAO (Decentralized Autonomous Organization), Tornado.Cash governance and mining smart contracts are deployed by its community.

The protocol also functions with zk-SNARK, which enables zero-knowledge proofs allowing users to demonstrate possession of information without needing to reveal it. The use of this technology is based **on open-source research made by Zcash team with the help of the Ethereum community**. To set up zk-SNARK initial keys, Tornado.Cash Trusted Setup Community was launched in May 2020 & accounts for 1114 contributions. This significant number of contributors makes it impossible to compromise the protocol by faking zero-knowledge proofs.

User interface is hosted on **IPFS** (InterPlanetary File System) by the community, minimizing risks of data deletion. Indeed, the interface will work as long as at least one user is hosting it.

EXHIBIT 121

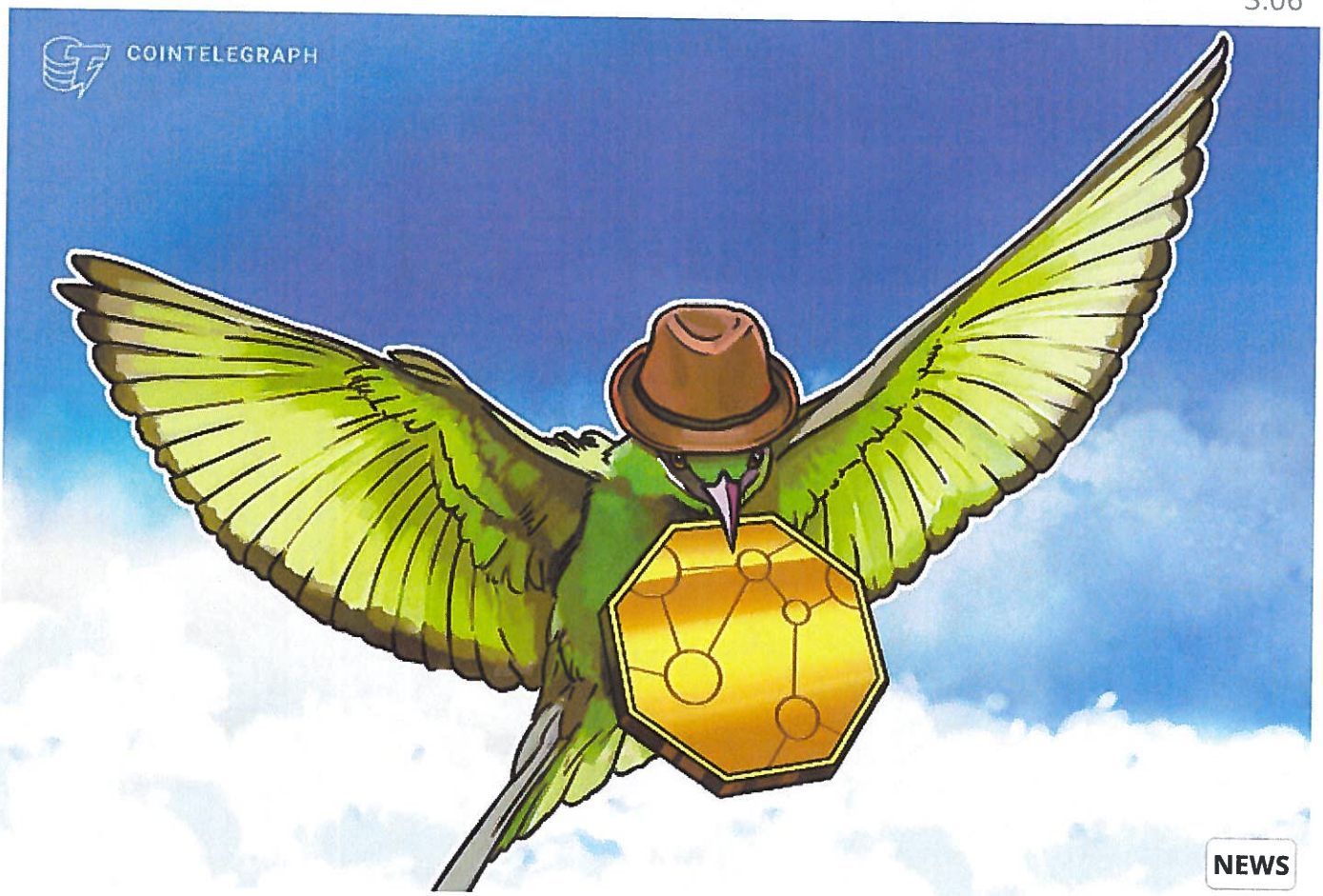
ANDREW THURMAN

FEB 09, 2021

TORN soars 200% as Tornado.Cash's governance token becomes tradable

Apes rejoice as yet another token airdrop fattens their portfolios

25470 31



The decentralizedfinance (DeFi) "stimulus checks" keep coming as Tornado.Cash joins Uniswap, Badger DAO, StakeDAO, and others in "airdropping" a now-tradable TORN governance token to early protocol participants.

Tornado Cash, which is an Ethereum "tumbling" service that obscures transactional history in order to preserve user privacy (as well as allowscammers and hackers a method to launder their funds), first announced the launch of a governance token in December. A snapshot for the airdrop was taken for Ethereum block 11400000, which was mined on December 6th, and

addresses which had interacted with the protocol prior to that point were entitled to an amount of TORN tokens weighted to the frequency and amount of Ether they used.

At current valuations, the distribution was one of the most lucrative for recipients to date. According to a post on community forums, the average recipient received 66.54 TORN tokens currently worth over $23,000, and the median user took in 21.24 tokens, worth $7500. The single largest recipient harvested over 2500 tokens worth a whopping $888,000.

The 500,000 airdropped tokens represent just 5% of the eventual 10,000,000 total TORN supply. The token had been locked as non-transferrable for 45 days, but that was released yesterday, and an additional 10% of the total supply is set aside for a "anonymity mining" program similar to liquidity mining.

Trading for the young token has been notably volatile. A liquidity pool on exchange aggregator and automated market maker (AMM) 1inch was established shortly after the token was unlocked, and TORN has a 24-hour high and low of $428 and $113, per Coingecko. At the time of writing the token currently trades at $350, and a pool has also been established on Uniswap.

Despite the airdrop bonanza, however, some have expressed skepticism that Tornado.Cash needs a governance token at all. The protocol currently works as intended, and the team transitioned the contracts to a state of immutability last year.

Additionally, in the governance announcement blogpost the team did not specify what the DAO treasury or team reserves — a combined total of 8,500,000 TORN tokens locked in a 3-5 year vesting schedule currently worth $3 billion — will be used for, only that through a DAO "the users of Ethereum will control their own privacy protocol."

In a Tweet from last year, Ethereum co-founder Vitalik Buterin seemed to echo this sentiment, saying that Tornado.Cash functions best as a "tool" rather than as an "ecosystem."

> Things like tornado cash and uniswap, kyber and the like are successful in part because they are just tools that people can put into their existing workflows, and not ecosystems. We need more tools that are content with being tools and fewer attempts at ecosystems
>
> — vitalik.eth (@VitalikButerin)February 18, 2020

Nonetheless, as asset valuations inflate across DeFi, this perhaps superfluous token drop likely won't be the last.

#Ethereum #Privacy #Tokens #Airdrop

What is Solana (SOL) Pay, and how does it work?

Q&A: Why cross-chain messaging matters

How blockchain can open up energy markets: EU DLT expert explains

What is StrongBlock (STRONG) and how does it work?

How to Keep Data Private With Google and Apple's Contact Tracing App

Incognito Blockchain Launches DeFi Privacy for Kyber

Are you a journalist or an editor? **Join us**

COINTELEGRAPH NEWSLETTER

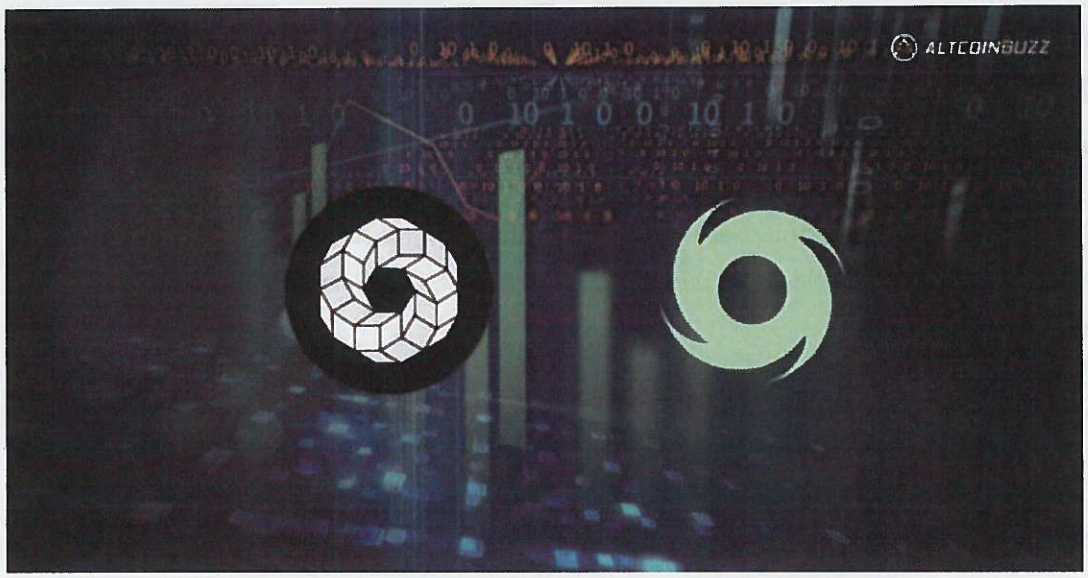
Email **Subscribe**

EXHIBIT 144

Make 61% APY With TORN on This Platform

Tornado Cash token holders can access an automated vault on PowerPool to compound staking earnings.

By **Martin Young** - May 11, 2022



Earning opportunities in decentralized finance are still plentiful despite the broader crypto market slump. This platform is offering more than 60% returns for staking certain tokens.

DeFi earnings platform PowerPool has announced a new vault for the Tornado Cash token, TORN. The protocol made the announcement that the ppTORN pool was live on May 10.

Furthermore, the new vault allows users to maximize TORN staking returns by utilizing PowerPool's auto-compounding algorithm. The vault uses a ppTORN smart contract that aggregates user deposits into the Tornado Cash governance staking contract.

Tornado Cash is a popular Ethereum mixing service that anonymizes transactions. Furthermore, the vault harvests and auto-compounds Tornado protocol fees for additional rewards.

> 💪+🎱 WE'RE HAPPY TO ANNOUNCE THAT NEW $PPTORN VAULT IS LAUNCHED. STAKE $TORN TO RECEIVE AUTO-COMPOUNDING REWARDS!
> 🎱 HTTPS://T.CO/FP0RX9L3LE
> 🎱 #PPTORN WAS AUDITED BY HTTPS://T.CO/D0EXZYI1CH

[redacted]

> 🎱 FIRST HARVEST HAS ALREADY BEEN EXECUTED!
> 🎱 $TORN COMMUNITY FEEDBACK UPGRADES 👉 SOON
>
> — POWERPOOL $CVP (@POWERPOOLCVP) MAY 10, 2022

More Than 60% APY

According to the announcement, the team calculated that during a two-month period, users generated 61% APY in the ppTORN vault. This is better than the 52% they earned for direct staking without the vault.

Additionally, users only pay the transfer fee and there is no fee for staking into the Tornado Cash contract, harvesting, or re-staking. To use the ppTORN vault, DeFi farmers need to do the following:

- Navigate to the app.powerpool.financewebsite,
- Click the "Vaults" section,
- Deposit TORN into the ppTORN vault, (needs wallet approval)
- Enjoy decent returns,
- Withdraw staked tokens when ready.

There was almost $100,000 in total value locked in thevault at the time of writing.

To develop the new DeFi product, the team ran experiments that processed on-chain data from the Tornado governance staking contract. A two-month test was run to estimate a staker's income in different scenarios with harvesting and re-staking.

"THE RESULTS REVEALED THAT PPTORN ALLOWS USERS TO GENERATE MORE INCOME WHILE REDUCING ETH GAS COSTS AND YIELD MANAGEMENT TIME."

It calculated that the ideal time frame for harvesting and re-staking was around 40 hours. Furthermore, PowerPool has automated all of the operations making the process very simple for TORN holders.

Additionally, there is no fixed lockup period so stakers can withdraw their initial deposit and rewards whenever they feel like it.

PowerPool has a mission to create and actively manage a diversified portfolio of automated, gas/capital-efficient, structuredDeFi product portfolios, and smart vaults.

TORN Price Outlook

The Tornado Cash token has made no gain over the last 24 hours. As a result, TORN was trading at $43.01 at the time of writing. However, the token has been battered with the rest of the crypto market this month.

TORN has slumped 15.8% over the past week and is down 90% from its February 2021 all-time high of $436.

The PowerPool Concentrated Voting Power token, CVP, has dropped 9.9% on the day to trade at $0.466. CVP has fallen even further from its all-time high.

Martin Young

Martin has been writing on Cybersecurity and Infotech for two decades. He has previous trading experience and has been covering the blockchain and crypto industry since 2017 for various publications.

EXHIBIT 154

Published in CENNZnet

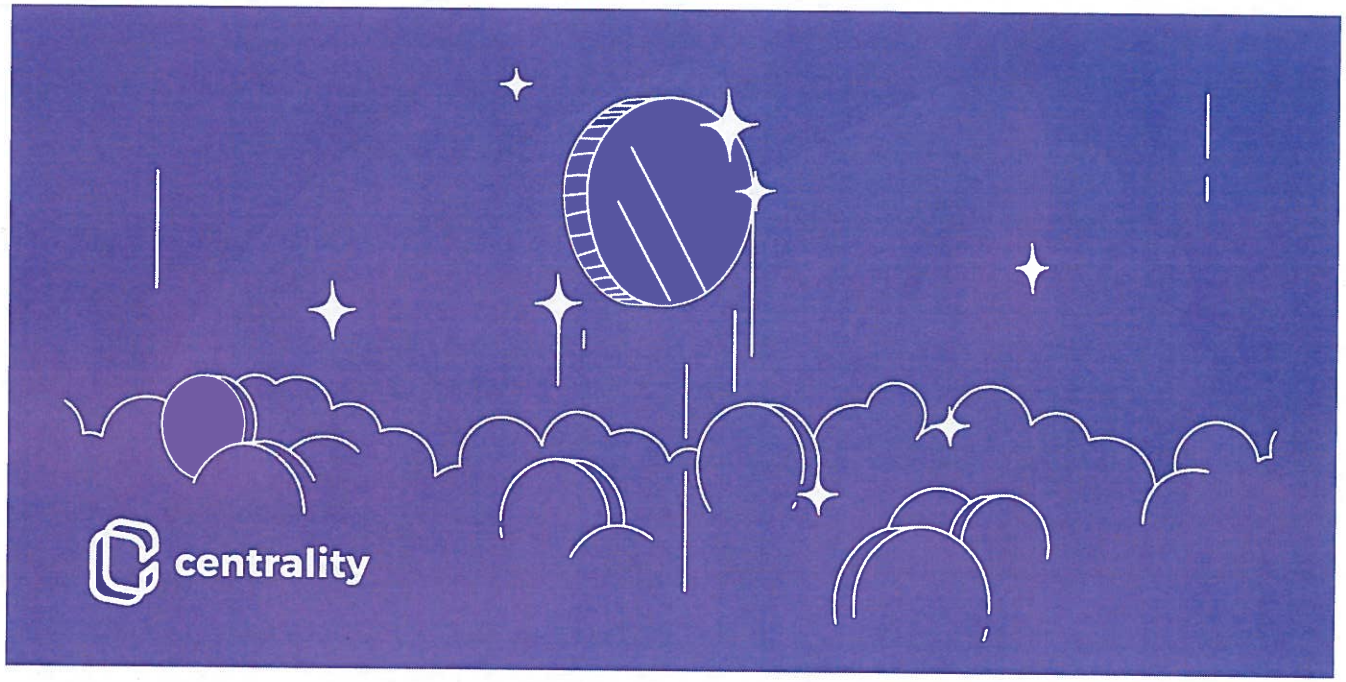
Cathy Breed Follow

Feb 25, 2021 · 4 min read · Listen

Validator node FAQ

Translations of this article can be found here:

- JP *Japanese version*
- CN *Chinese version*



What are Validators?

On CENNZnet we have two roles within staking: Validators and Nominators. Validators are node operators who each store a copy of the blockchain and must perform certain functions to keep the system secure. On CENNZnet validator nodes are responsible for authoring new blocks and voting in the finalization protocol.

CENNZnet will have 12 validator slots at launch — but this number will increase as the network matures and governance decisions are made.

To learn more check out our detailed guide to staking on CENNZnet here.

Why are validators important to CENNZnet?

Validators are an essential part of the Proof of Stake consensus mechanism. They are essentially the moderators of the staking system and have the extremely important job of authoring new blocks on the chain.

To have the most decentralised system possible, CENNZnet needs a good number of different Validator nodes that can be elected. This makes for the greatest variety of staking options for the community and also protects the system by preventing the chain from being controlled by one very wealthy individual. For example, if there are few Validators, one person with a reasonable amount of CENNZ could take all the Validator nodes, therefore taking complete control of the chain. When there are more people Validating it significantly increases the barrier to being elected.

Validator nodes can be run by anyone with hardware that meets the minimum requirements (250G storage 8G RAM).

However, it is important to remember that if a Validator fails to uphold their responsibilities a portion of their stake will be slashed (fined). If you are unsure about taking on the technical responsibility of Validating just yet, you can get to grips with the staking process as a Nominator first.

The responsibilities of a Validator are:

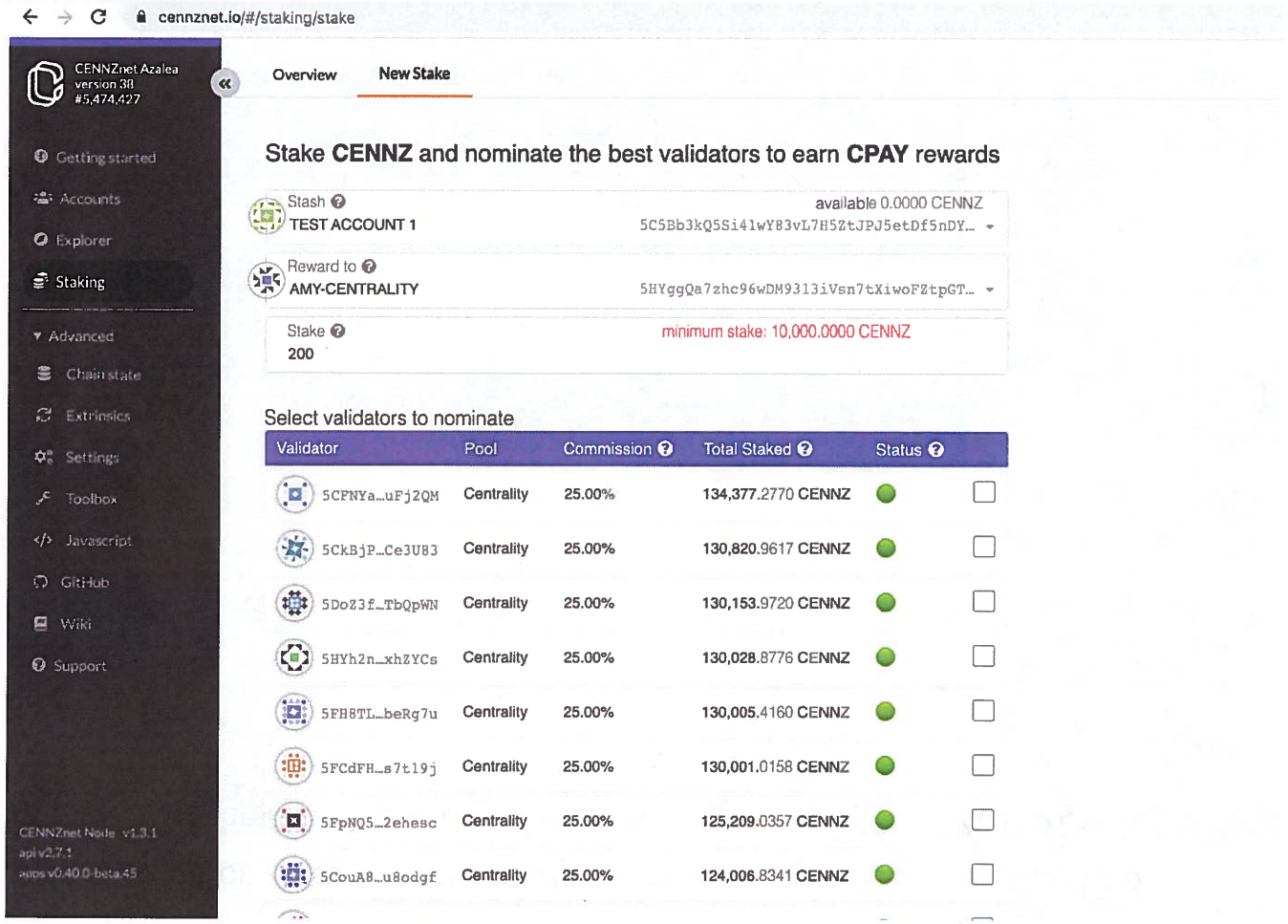
- Run a node.
- Stake a minimum 10,000 CENNZ.
- Produce blocks. This requires your node to be online before the elected era to sync to the latest blocks, and be online 24/7 for the elected eras.

You can learn more about how to set up a Validator node on our Github page here.

What is a validator's commission rate?

percentage of the pooled stake reward. It is up to the individual Validator how much of a percentage they wish to take. Nominators can check commission rates before they choose a Validator.

The commission rates that the validators charge are available in the list of validators in the New Stake tag of the Staking page on CENNZnet.io.



What is an oversubscribed Validator?

Validators can only pay out CPAY rewards to a certain number of nominators per

(ranked by amount staked by each nominator) are paid rewards. Other nominators will receive no rewards for that era, although their stake will still be used to calculate entry into the active validator set.

Why are most of the validator nodes run by Centrality?

To get the staking process started we needed 12 robust Validator nodes fully set up and ready to go. To bootstrap staking, Centrality has taken 9 Validator nodes. This is just a temporary situation while more people start joining as Validator nodes. In the long term, we aim to make the network as decentralised as possible, which means more independent Validators joining the network to provide a variety staking options for our Nominator community and security.

Why do the Centrality validators have 25% commission?

As mentioned above, Centrality's aim is to encourage other Validators to join the network and be elected. We do not want to be the default staking Validator node as this is not good for the decentralisation of the network.

Having a very high commission on our Validator nodes provides an incentive for

Why are there only 12 validator nodes an era?

This is only the initial number of Validators required for a staking era. As CENNZnet grows, we will have more validators in the network. It will be up to governance to decide how many validators we want to list.

Can you run more than one Validator node?

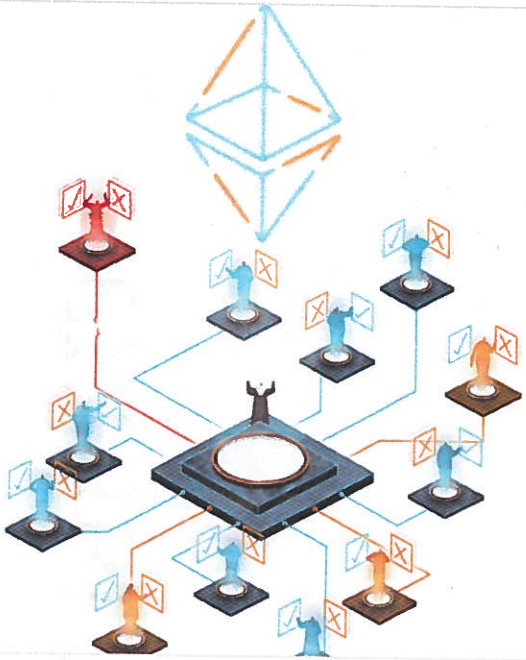
You can run as many Validator nodes as you have the capacity to. You can set up validator nodes to run on the cloud so that you don't need to maintain the physical hardware. The CENNZnet team plans to provide scripts to automate this in the future.

Where can I get support?

Support for Validators can be found on our Discord channel here.

To stay up-to-date on the progress of our technology, follow us on Twitter, Telegram,

EXHIBIT 157



Decentralized autonomous organizations (DAOs)

- Member-owned communities without centralized leadership.
- A safe way to collaborate with internet strangers.

- [redacted]lace to commit funds to a specific cause.

On this page

Ethereum use cases

DAOs are an effective and safe way to work with like-minded folks around the globe.

Think of them like an internet-native business that's collectively owned and managed by its members. They have built-in treasuries that no one has the authority to access without the approval of the group. Decisions are governed by proposals and voting to ensure everyone in the organization has a voice.

There's no CEO who can authorize spending based on their own whims and no chance of a dodgy CFO manipulating the books. Everything is out in the open and the rules around spending are baked into the DAO via its code.

Why do we need DAOs?

Starting an organization with someone that involves funding and money requires a lot of trust in the people you're working with. But it's hard to trust someone you've only ever interacted with on the internet. With DAOs you don't need to trust anyone else in the group, just the DAO's code, which is 100% transparent and verifiable by anyone.

This opens up so many new opportunities for global collaboration and coordination

p so many new opportunities for global collaboration and coordination.

A comparison

DAO	A traditional organization
Usually flat, and fully democratized.	Usually hierarchical.
Voting required by members for any changes to be implemented.	Depending on structure, changes can be demanded from a sole party, or voting may be offered.
Votes tallied, and outcome implemented automatically without trusted intermediary.	If voting allowed, votes are tallied internally, and outcome of voting must be handled manually.
Services offered are handled automatically in a decentralized manner (for example distribution of philanthropic funds).	Requires human handling, or centrally controlled automation, prone to manipulation.
All activity is transparent and fully public.	Activity is typically private, and limited to the public.

DAO examples

To help this make more sense, here's a few examples of how you could use a DAO:

- A charity – you can accept membership and donations from anyone in the world and the group can decide how they want to spend donations.
- A freelancer network – you could create a network of contractors who pool their funds for office spaces and software

subscriptions.

- Ventures and grants – you could create a venture fund that pools investment capital and votes on ventures to back. Repaid money could later be redistributed amongst DAO-members.

DAO membership

There are different models for DAO membership. Membership can determine how voting works and other key parts of the DAO.

Token-based membership

Usually fully permissionless, depending on the token used. Mostly these governance tokens can be traded permissionlessly on a decentralized exchange. Others must be earned through providing liquidity or some other 'proof-of-work'. Either way, simply holding the token grants access to voting.

Typically used to govern broad decentralized protocols and/or tokens themselves.

A famous example

MakerDAO↗ – MakerDAO's token MKR is widely available on decentralized exchanges. So anyone can buy into having voting power on the Maker protocol's future.

Share-based membership

Share-based DAOs are more permissioned, but still quite open. Any prospective members can submit a proposal to join the DAO, usually offering a tribute of some value in the form of tokens or work. Shares represent direct voting power and ownership. Members can exit at any time with their proportionate share of the treasury.

Typically used for more closer-knit, human-centric organizations like charities, worker collectives, and investment clubs. Can also govern protocols and tokens as well.

A famous example

MolochDAO ↗ – MolochDAO is focused on funding Ethereum projects. They require a proposal for membership so the group can assess whether you have the necessary expertise and capital to make informed judgments about potential grantees. You can't just buy access to the DAO on the open market.

How do DAOs work?

The backbone of a DAO is its smart contract. The contract defines the rules of the organization and holds the group's treasury. Once the contract is live on Ethereum, no one can change the rules except by a vote. If anyone tries to do something that's not covered by the rules and logic in the code, it will fail. And because the treasury is defined by the smart contract too that means no one can spend the money without the group's approval either. This means that DAOs don't need a central authority. Instead, the group makes decisions collectively, and payments are automatically authorized when votes pass.

This is possible because smart contracts are tamper-proof once they go live on Ethereum. You can't just edit the code (the DAOs rules) without people noticing because everything is public

out people noticing because everything is public.

More on smart contracts →

Ethereum and DAOs

Ethereum is the perfect foundation for DAOs for a number of reasons:

- Ethereum's own consensus is distributed and established enough for organizations to trust the network.
- Smart contract code can't be modified once live, even by its owners. This allows the DAO to run by the rules it was programmed with.
- Smart contracts can send/receive funds. Without this you'd need a trusted intermediary to manage group funds.
- The Ethereum community has proven to be more collaborative than competitive, allowing for best practices and support systems to emerge quickly.

Join / start a DAO

Join a DAO

- Ethereum community DAOs
- DAOHaus's list of DAOs↗

Start a DAO

- Summon a DAO with DAOHaus ↗
- Create an Aragon-powered DAO ↗
- Start a colony ↗
- Build a DAO with DAOstack ↗

Further reading

DAO Articles

- What's a DAO? ↗ – Aragon ↗
- House of DAOs ↗ – Metagame ↗
- What is a DAO and what is it for? ↗ – DAOhaus ↗
- How to Start a DAO-Powered Digital Community ↗ – DAOhaus ↗
- What is a DAO? ↗ – Coinmarketcap ↗

Videos

- What is a DAO in crypto? ↗

Website last updated: April 25, 2022

Use Ethereum

Ethereum wallets

Get ETH

Decentralized applications (dapps)

Layer 2

Run a node

Stablecoins

Stake ETH

Learn

What is Ethereum?

What is ether (ETH)?

Community guides and resources

History of Ethereum

Ethereum Whitepaper

Ethereum upgrades

Ethereum security and scam prevention

Ethereum glossary

Ethereum governance

Blockchain bridges

Developers

Get started
Documentation

Tutorials

Learn by coding

Set up local environment

Enterprise

Mainnet Ethereum

Private Ethereum

Enterprise

Ethereum energy consumption

What is Web3?

Ethereum Improvement Proposals

Ecosystem

Community hub
Ethereum Foundation

Ethereum Foundation Blog ↗

Ecosystem Support Program ↗

Ecosystem Grant Programs

Ethereum brand assets

Devcon ↗

About ethereum.org

About us

Jobs

Contributing

Language support

Privacy policy

Terms of use

Cookie policy

Contact ↗

EXHIBIT 176

DEFI

Tornado Cash Token (TORN) Surges 94% Following Bullish Protocol Updates

M 2022, 9:3 AM AEST · s ago
Jody McDonald
Crypto News Writer

The native token for the Tornado Cash protocol (TORN), an Ethereum-based privacy protocol, has surged 94 percent following the launch of its latest network updates.

Tornado Cash is a fully decentralised privacy protocol which enables anonymous transactions on the Ethereum network. The protocol achieves anonymity primarily by breaking the on-chain link between source and destination addresses when transactions are made.

> I have seen a bit of @TornadoCash hate recently. This is ridiculous. There are many reasons other than crime that a person would want privacy. Here is a short list.
>
> — 0xcacti (@0xcacti) February 14, 2022

Price Increase Follows Launch Of Relayers

The latest price action for TORN follows the adoption and implementation of the protocol's 10th on-chain governance proposal, which saw the addition of relayers to the network:

> @TornadoCash relayer registry proposal #10 is definitely bullish for $TORN holders 🚀📈
> With the latest governance proposal about to be validated, I'm making a point about why this is so beneficial to $TORN valuation.
> ⬇️⬇️⬇️⬇️⬇️⬇️
> — bt11ba (@bt11ba) February 16, 2022

The community voted overwhelmingly in favour of the proposal, which was accepted on February 19. Following the launch of relayers on March 2, the price of TORN spiked from around US$37 to around the $US67 mark.

What Are Relayers?

Tornado Cash relayers are community members who process withdrawal transactions and allow users to send transactions to accounts with no ETH balance – they are considered an important part of the protocol and improve users' privacy.

Relayers are compensated for their network services with a small portion of users' deposits. Anyone can become a relayer, provided they meet the minimum balance requirement of 300 TORN and accept the terms and conditions.

TORN Gaining Momentum

The addition of relayers to the Tornado Cash protocol is a further boost following its integration of ETH layer 2 solution Arbitrum in December 2021, which saw a dramatic decrease in gas fees and improvements in transaction times:

> 4/4 📋 Final Score: 85% 🔥 #DeFi #ETH #MATIC #AVAX #BSC $TORNhttps://t.co/4Fs1fQ8uRK@semenov_roman_ @TornadoCash @bt11ba @WUTornado @rstormsf @WillMcTighe @kaili_jenner @mike_h_wu
> — DeFiSafety (@DefiSafety) March 1, 2022

The protocol was also recently assessed by DeFi safety, which found it to be highly secure – awarding Tornado Cash an overall score of 85 percent.

Top ↑

DEFI ETHEREUM (ETH) PRIVACY TORNADO CASH (TORN)

Share this article

Join in the conversation on this article's Twitter thread.

Disclaimer: The content and views expressed in the articles are those of the original authors own and are not necessarily the views of Crypto News. We do actively check all our content for accuracy to help protect our readers. This article content and links to external third-parties is included for information and entertainment purposes. It is not financial advice. Please do your own research before participating.

Related News

DEFI

DeFi needs appropriate regulation before moving to retail, says Fed Chair: Finance Redefined

4 hours ago by Cointelegraph

NFTS

Starfish Finance Proposes DeFi-NFT Convergence on Polkadot

4 hours ago by Usethebitcoin

Trusted Partners

Trending

RIPPLE #1
Popular Crypto Analyst Doubles Down on Explosive $XRP Price Prediction

BITCOIN #2
Markets: XRP jumps amid court ruling against SEC, Bitcoin gains, Ether sole loser in crypto top 10

TERRA #3
Crypto Trader Says One Altcoin That's Exploded 120% This Month Is About To Nuke – Here's His Target

Popular

Top ↑

REVIEW
The Best Crypto Exchanges for Australia

EVENT
Australia Crypto Convention - Gold Coast, Sep 2022

Today's Top Gainers

SAFEMOON	$8.39	▲57.72%
LUNC	$0.00	▲6.09%
ONT	$224.0	▲5.91%
FX	$0.38	▲5.24%
HNT	$8.39	▲5.12%
TON	$2.10	▲4.72%

View more powered by Swyftx.com.au

Top Daily News

Your email address Go

Real-Time News

Follow on Twitter

Join on Telegram

Subscribe on Google News

AUSTRALIA

Crypto News provides you with the most relevant Bitcoin, cryptocurrency & blockchain news.

Useful links
- News Archive
- Sponsored Articles
- Institution Crypto Purchases
- Crypto Whale Transactions

About Us
- About
- Writers
- Partners
- Affiliates
- Advertise
- Contact

Are you a journalist or an editor? Join us: editor@cryptonews.com.au

Top ↑